

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problems Mailbox.**

THIS PAGE BLANK (USPTO)



19 BUNDESREPUBLIK
DEUTSCHLAND



DEUTSCHES
PATENTAMT

12 Offenlegungsschrift
10 DE 195 34 529 A 1

61 Int. Cl.⁸:
G 07 B 17/04
G 06 F 12/14

21 Aktenzeichen: 195 34 529.0
22 Anmeldetag: 8. 9. 95
43 Offenlegungstag: 13. 3. 97

DE 195 34 529 A 1

71 Anmelder:
Francotyp-Postalia AG & Co., 16547 Birkenwerder,
DE

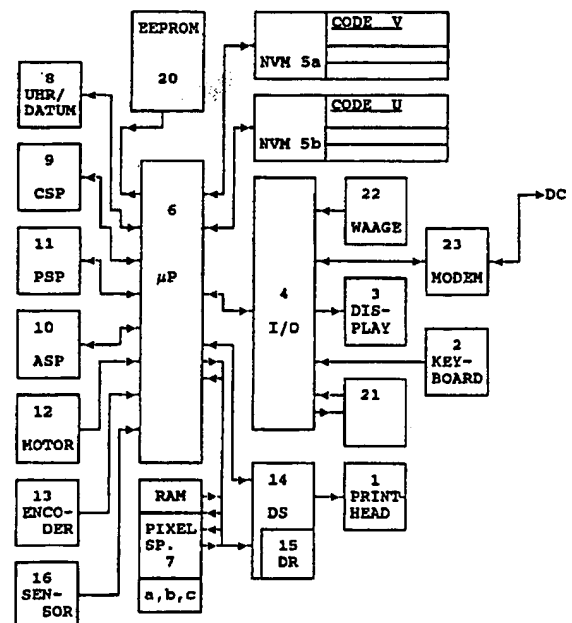
72 Erfinder:
Kubatzki, Ralf, 10405 Berlin, DE; Thiel, Wolfgang,
Dr., 13503 Berlin, DE

56 Entgegenhaltungen:
US 51 24 926
US 44 47 890
EP 02 31 452 A2

Prüfungsantrag gem. § 44 PatG ist gestellt

54 Verfahren und Anordnung zur Erhöhung der Manipulationssicherheit von kritischen Daten

- 57 Ein Verfahren zur Erhöhung der Manipulationssicherheit von kritischen Registerdaten umfaßt die Schritte:
- Laden einer Zahl oder eines Zeigers, welcher einem Codewort zugeordnet ist, in einen ersten nichtflüchtigen Speicher 20,
 - Laden eines Codewortes in zweite die Postregisterdaten enthaltenden nichtflüchtigen Speicher (NVM 5a, 5b), wobei das Codewort dem letzten Betriebszustand der Frankiermaschine zugeordnet ist, d. h. das dem Ergebnis der Herstellung oder einer Nachladung der Frankiermaschine bzw. vor dem Ausschalten bzw. vor Spannungsausfall oder vor einer Stillstandszeit (Stand by) bzw. vor Programmunterbrechung entsprechend ausgewählt worden ist,
 - Gültigkeitsprüfung des Codewortes mindestens zum Zeitpunkt des Einschaltens der Frankiermaschine und
 - Ersetzen des alten Codewortes durch ein vorbestimmtes neues Codewort, wenn der Prozessor, nach Gültigkeitsprüfung mit Bezug auf das in seinem internen Prozessorspeicher (NVM 6c) aus einer Liste mit gespeicherten Codewörtern entsprechend der Zahl bzw. der Zeigerstellung ausgewählte Codewort, die Gültigkeit des alten Codewortes erkennt oder
 - Blockierung der Frankiermaschine nach dem Zeitpunkt des Einschaltens der Frankiermaschine, wenn der Prozessor nach Gültigkeitsprüfung mit Bezug auf das ausgewählte in vorgenannter Liste gespeicherte Codewort die Gültigkeit des alten Codewortes aberkennt.



DE 195 34 529 A 1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

BUNDESDRUCKEREI 01. 97 602 071/443

28/25

Die Erfindung betrifft ein Verfahren und Anordnung zur Erhöhung der Manipulationssicherheit von kritischen Daten, welche in informationsverarbeitenden Einrichtungen vor einer Manipulation geschützt werden müssen, insbesondere von kritischen Registerdaten in elektronischen Frankiermaschinen oder in einer anderen elektronischen Einrichtung, in welcher sicherheitsrelevante Daten gehandelt werden bzw. in der eine Abrechnung von geldwerten Daten vorgenommen wird.

Frankiermaschinen sind, mit mindestens einem Eingabemittel, einem Steuermodul und einem Druckermodule ausgerüstet. In einem Speichermittel werden nichtflüchtig Daten gespeichert, welche zum Betrieb der Frankiermaschine erforderlich sind sowie Daten, welche Geldmitteln entsprechen.

Die Frankiermaschinentypen unterscheiden sich in Form und Ausstattung entsprechend des zu bearbeitenden Postaufkommens. Sollen aber verschiedene Typen an Frankiermaschinen produziert werden dann müssen eine Vielzahl an Schaltkreisen (ASIC's oder/und andere Bauelemente) vorgesehen werden. Gerade die Vielzahl an Bauelementen und Schaltkreisen bietet dann Ansatzpunkte für eine Manipulation, wenn kein alternativer Aufwand getrieben oder ein Sicherheitsgehäuse eingesetzt wird.

Aus dem EP 465 236 A2 ist ein ASIC bekannt, welches eine Schaltung zur Drucksteuerung zur Motorsteuerung und zur Abrechnung umfaßt. Die Schaltung zur Drucksteuerung umfaßt einen Speicher für feste und einen anderen für variable Daten, welche mit den festen Daten überlagert werden. Ein Motorcontroller ist für ein Aktivieren eines Motorantriebes in Abhängigkeit von der Poststückzuführung vorgesehen. Ein Vorteil ist zweifellos die hohe Manipulationssicherheit aufgrund der Verwendung eines einzigen ASIC, d. h. resultierend allein bereits aus der eingeschränkten Anzahl an Ansatzpunkten für eine Manipulation. Ein Nachteil der Verwendung eines einzigen ASICs ist die schlechte Verwendbarkeit für unterschiedliche Frankiermaschinen, welche einen unterschiedlichen Drucker und Steuermodul entsprechend eines realisierten Frankiermaschinensystem bzw. Poststraße aufweisen.

Aus der US 4 858 138 ist ein modulares System für eine Frankiermaschine mit Meter/Base-Trennung bekannt, wobei ein Sicherheitsmodul (Meter) mit einem Drucksteuermodul (Base) gekoppelt ist. Das Sicherheitsmodul kann Kreditkartenform aufweisen. Als elektrische Verbindungseinrichtung zum Drucksteuermodul dient hierbei ein als parallele CPU-Schnittstelle ausgebildeter Hochgeschwindigkeitskommunikationsbus. Der Drucksteuermodul weist einen Hochgeschwindigkeitsdrucker auf. Von der Tastatur des Drucksteuermoduls eingegebene Portobetrag wird zum Sicherheitsmodul übertragen. Der Sicherheitsmodul liefert eine digitale Darstellung des festen Teils des Postwertzeichens und eine verschlüsselte Gültigkeitsnummer. Die Gültigkeitsnummer umfaßt den Portobetrag und ggf. weitere Informationen, wie die Frankiermaschinenseriennummer und das Datum. Die verschlüsselte Gültigkeitsnummer ist geeignet, um ein illegales Drucken eines Geldbetrages, der nicht berechnet wurde, festzustellen. Die Fälschungssicherheit beruht auf einer in einer Sicherheitslogik vorgenommenen Verschlüsselung einer Gültigkeitsnummer, die über eine CPU-Schnittstelle übertragen wird. Diese Lösung bringt aber keinen Vorteil bei Manipulationen, welche im Sicherheitsmodul bzw. am

Bus zwischen den Postwertspeichern und der Sicherheitslogik vorgenommen werden. Ein Nachteil ist hier, daß als einziger Schutz nur das Sicherheitsgehäuse des Sicherheitsmoduls vorgesehen ist. Nachteilig ist auch die hohe Anzahl der Leitungen der Meter/Base-Verbindung an der Schnittstelle zur Base und daß eine teure Hochgeschwindigkeitsschnittstelle erforderlich ist.

Eine weitere Manipulationsmöglichkeit besteht während der Dateneingabe beim Nachladen der Frankiermaschine mit einem Guthaben. In üblicher Weise wird von einer Datenzentrale bzw. von einem Speicher eines Übertragungsmittels, vorzugsweise einer Chipkarte, ein Guthaben geladen. Davon werden die durch die Frankiermaschine verbrauchten Portobeträge abgebucht.

Zur Sicherheit gegen betrügerische Manipulationen ist bereits weiterhin aus der DE 38 23 719 bekannt, ein repräsentatives Zeichenmuster ab einem bestimmten Datum auszudrucken. Bei der Prüfung der Post wird im Postamt das Druckdatum und das Zeichen mit dem Muster verglichen, das für dieses Datum berechtigt ist. Zum Drucken dient eine Berechtigungsvorrichtung, die eine Speichervorrichtung zur Speicherung einer Anzahl Zeichenmuster- und Datumsdaten aufweist. Die Daten, die das repräsentative Zeichenmuster einem definierten Datum zuordnen, werden über eine Fernwertvorgabe mittels einer externen Wahlvorrichtung dann aktualisiert, wenn die Anwender der Frankiermaschinen um eine Rekreditierung nachsuchen. Die Sicherheit der Daten beruht auf dem Prüfen der Daten in der Datenzentrale bevor ein Nachladen erfolgt und im Prüfen der Frankierabdrucke seitens der Postbehörde. Die Datenzentrale trägt somit zur Erhöhung der Manipulationssicherheit von kritischen Registerdaten bei. Dieses Sicherheitssystem ist jedoch auf Festnetze beschränkt und für tragbare Frankiermaschinen, die von einem Ort zu einem anderen Ort mitgeführt werden (mobiles Büro) nicht anwendbar. Eine Selbstprüfung seitens der Frankiermaschine auf Manipulation ist nicht vorgesehen.

Einer Portogebührentabelle ist die für das Poststück erforderliche Portogebühr entnehmbar. Der Portorechner, welcher aus dem Gewicht des Poststückes den gültigen Portobetrag bestimmt, ist gewöhnlich bereits in der an die Frankiermaschine angeschlossenen Waage integriert. Jedoch wurden auch schon Lösungen mit einem in die Frankiermaschine integrierten Portorechner vorgeschlagen.

Beispielsweise weist eine aus der DE 42 13 278 A1 bekannte transportierbare Frankiermaschine Speichermittel und mit diesen in Verbindung stehende Empfangsmittel für über ein Übertragungsmittel übertragbare Daten auf. Das Speichermittel der Frankiermaschine weist aktualisierbare Abschnitte für an bestimmte Bedingungen geknüpfte Tabellen auf, beispielsweise für mindestens eine aktuelle Portogebührentabelle, anhand derer die jeweilige Portogebühr ermittelt wird. Die Frankiermaschine weist im Steuermodul erste Mittel auf, die bei Inbetriebnahme der Frankiermaschine mindestens eine Portogebührentabelle für die Frankiermaschine aus dem Speicher des Übertragungsmittels über die Empfangsmittel in einen vorbestimmten Speicher des Speichermittels laden. Sie enthält zweite Mittel im Steuermodul, die mittels der über dritte Mittel eingegebenen Bedingungen anhand des bereits eingegebenen Absendelandes bzw. -ortes und des Datums die aktuelle in Kraft befindliche Portogebührentabelle auswählen, um diese zu laden. Diese ersten und zweiten Mittel sind hardware- und/oder softwaremäßig als ein fest- oder freiprogrammierbarer Logikmodul bzw. Pro-

gramm einer Mikroprozessorsteuerung ausgebildet und bewirken bei jedem Einschalten eine Verbindungsaufnahme zum externen Speicher.

Solche aktualisierbaren Abschnitte des Speichermittels sind ebenfalls für andere Informationen und/oder Zusatzinformationen vorgesehen. Insbesondere kann die Sicherheit vor betrügerischen Manipulationen dadurch erhöht werden, daß bei der Aktualisierung eine dem Aktualisierungsdatum zugeordnete Anzahl von Funktionen in die Frankiermaschine ladbar sind und die weiteren zu ladenden auslösbaren Funktionen vielfältig und nicht wählbar vorgegeben sind. Zur Sicherheit gegen betrügerische Manipulationen kann von der nationalen Postbehörde, zu der der jeweilige Absendeort gehört, ein nur von der jeweiligen nationalen Postbehörde maschinenlesbarer Ausdruck vorgegeben sein. Dieser Ausdruck kann beispielsweise die Transaktionsnummer für eine Berechtigungsprüfung in Strichcodedarstellung sein oder ein anderes vereinbartes Zeichen, welches unter Verwendung des gleichen oder weiteren Druckers an einer definierten Stelle auf dem Postgut abgedruckt wird.

Solche Sicherheitsmaßnahmen sind geeignet den Einsatz eines Farbkopierers zur unerlaubten Vervielfältigung eines Frankierabdruckes zu vereiteln. Sie können jedoch nicht die innere Manipulationssicherheit der Daten in der Frankiermaschine erhöhen.

Damit nicht die Speicherinhalte geklont wiederverwertet werden, müßte aber die Abrechnungseinheit wieder mit einem Sicherheitsgehäuse ausgerüstet werden. Andererseits ist dann aber dadurch weiterhin der Austausch defekter Bauelemente erschwert.

In der EP 560 714 A2 sind die Montageeinheiten durch ein Sicherheitsgehäuse gekapselt. Zur fälschungssicheren Übertragung von Abrechnungsdaten von einem Speicher in einer defekten Montageeinheit auf den Speicher einer in die Frankiermaschine neu eingesetzten Montageeinheit wird jede Montageeinheit mit zwei Steckereinheiten ausgerüstet. Zunächst wird der Datenfluß durch eine besondere Übertragungsleitung einer ersten Steckereinheit geschlaucht, wobei aber an der gleichen ersten Steckereinheit der alten Montageeinheit die Schlaufung entfernt und der normale Datenfluß unterbrochen und umgeleitet ist. Vom Speicher der alten Montageeinheit wird über die letztgenannte Steckereinheit und mittels einer zweiten Steckereinheit der neuen Montageeinheit der Datenfluß auf die neue Montageeinheit umgeleitet. Es sind mechanische Verriegelungsglieder vorgesehen, welche in Wirkverbindung mit einem elektronischen Erkennungsmerkmal (Flag) setzenden Schalters stehen, welcher beim Herausnehmen der defekten Montageeinheit betätigt wird. Nach dem Übertragen der Daten auf die neue Montageeinheit wird ein zweites unlösbares Flag gesetzt, so daß eine zweite Datenübertragung unmöglich gemacht ist. Die Sicherheit beruht im wesentlichen auf der Kapselung von CPU und nichtflüchtigem Speicher auf der Montageeinheit und dem vorgenannten Schalter zum Setzen der Flags. Bei Kenntnis der Lage bzw. Anordnung des Schalters kann ein Eindringen und eine Manipulation in Fälschungsabsicht aber nicht verhindert werden.

Aus der DE 41 29 302 A1 ist die Verwendung eines Sensors bekannt, welcher beim Öffnen des Frankiermaschinengehäuses die Postregister löscht. Jedoch kann damit nicht verhindert werden, daß neue Daten in das Postregister von einem geschickten Manipulator eingeschrieben werden können, wenn das Gehäuse erst einmal geöffnet ist.

Aus der EP 231 452 A2 ist das periodische Abfragen von Sensoren entsprechend einer Software routine einer CPU bekannt. Der Nachteil dieser Lösung besteht in einer hohen Rechenzeit bedingt durch das periodische Abtasten der Sensoren. Dieser Nachteil wird noch vergrößert, wenn es sich um eine besonders zeitkritische Abfrage handelt. Um möglichst schnell auf eine Zustandsänderung reagieren zu können, muß die Abfragefrequenz hoch gewählt werden. Somit verbringt der Mikroprozessor einen großen Anteil seiner Rechenzeit mit der Abfrage. Außerdem kann nicht die Manipulation einer ausgeschalteten Maschine verhindert werden.

Es wurde bereits in der DE 42 17 830 A1 ein Verfahren zum Betreiben einer Datenverarbeitungsanlage mit einem ersten nichtflüchtigen Speicher, einem Zustandsspeicher und einem zweiten nichtflüchtigen Speicher vorgeschlagen. Eine Modulkennung ermöglicht die Fortsetzung des Programms und eine Zustandskennung ermöglicht die Bearbeitung und Fortsetzung des Programmabschnitts bei dem eine Programmunterbrechung eintrat, d. h. ggf. die Korrektur fehlerhaft eingeschriebener Daten in einem NVM aufgrund redundant vorliegender Daten in dem anderen NVM. Diese Lösung kann aber nicht den Dateninhalt, auf Vorliegen einer Manipulation überprüfen. Beim Klonen von Speicherinhalten werden korrekte Daten auf externe Speicher überspielt. Beim Rückübertragen dieser Speicherinhalte bzw. beim Einsatz dieser externen Speicher in die Frankiermaschine zu einem späteren Zeitpunkt wird ein von der Frankiermaschine selbst nicht als fehlerhaft erkennbarer Zustand wiederhergestellt, der zu einem früheren Zeitpunkt einmal korrekt war.

Es ist bereits ein Verfahren zur Verbesserung der Sicherheit von Frankiermaschinen vorgeschlagen worden (DE 43 44 476 A2) indem die Frankiermaschine zwischen autorisierten und unautorisierten Eingriff bzw. Öffnen ihres Gehäuses unterscheiden kann. Das Verfahren setzt aber voraus, daß die Frankiermaschine ständig mit Energie für die Selbstprüfung versorgt wird. In diesem Fall können keine sicherheitsrelevanten Daten aus der Frankiermaschine unerlaubt herausgeladen, abgenommen oder eingespeist werden, ohne daß dies im Rahmen der Selbstprüfung bemerkt würde. Dennoch sind zusätzliche Gehäuse, Siegel und/oder weitere Sicherheitsmaßnahmen erforderlich zum Schutz der ausgeschalteten Maschine.

Vielfach wird die Forderung erhoben, daß für Reparaturzwecke die Speicherbausteine leicht austauschbar sind, also weder gekapselt noch fest eingelötet sondern gesockelt werden. Nun wäre es damit aber nicht möglich, die tragbaren, d. h. die nicht fest über ein Telefonnetz installierten Frankiermaschinen im ausgeschalteten Zustand gegenüber betrügerischen Manipulationen abzusichern. Im Interesse der Manipulationssicherheit von kritischen Registerdaten muß bisher auf Verbesserungen beim Service für die Maschine verzichtet werden.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren zur Erhöhung der Manipulationssicherheit von kritischen Registerdaten zu entwickeln, welche die Nachteile des Standes der Technik vermeidet und für eine Vielzahl an Frankiermaschinenvarianten kostengünstig realisierbar ist, ohne dabei die Manipulationssicherheit zu vermindern.

Eine weitere Aufgabe ist es, bei einer Anordnung zum Frankieren von Postgut, vorzugsweise einer tragbaren ortsunabhängig betreibbaren Frankiermaschine der eingangs genannten Gattung eine Sicherheit gegen be-

trügerische Manipulationen jeder Art und ein Frankieren nach gültigen Posttarifen in Abhängigkeit von dem eingebaren Gewicht und Format des Postgutes zu gewährleisten. Auch bei ausgeschalteter Frankiermaschine und ohne Stromversorgung soll die frankiermaschineninterne Sicherheitsschaltung für Postregisterdaten und andere sicherheitsrelevante Daten wirksam sein.

Die Aufgabe wird mit den Merkmalen der Ansprüche 1, 10, 15 bzw. 16 gelöst.

Die Erfindung geht davon aus, daß ein Duplizieren bzw. Klonen des zu schützenden NVMs nicht verhindert werden braucht, sondern auch ein Duplikat des Speicherinhalts, welches gegen den Speicherinhalt des Originals ausgetauscht wird, weiterverwendet werden kann. Im Reparaturfall wird oft ein Kopieren und Rücktausch der Speicherinhalte erforderlich, wobei allerdings vorausgesetzt wird, daß zwischenzeitlich keine gültigen Frankierungen vorgenommen werden.

Erfindungsgemäß wird ein interner Prozessorspeicher verwendet, um ein Codewort nichtflüchtig zu speichern.

Es ist vorgesehen, daß jedem nichtflüchtigem Speicher oder Speicherbereich ein separates Codewort zugeordnet wird, wobei mindestens eines der vorgenannten separaten Codewörter in einem weiteren internen Speicher eines Prozessorsystems, einer Chipkarte und/oder einer Datenzentrale nichtflüchtig gespeichert worden ist und daß eine Bildung von neuen Codewörtern ab einem vorbestimmten Zeitpunkt und danach eine Einspeicherung der neuen Codewörtern in nichtflüchtigen Speichern vorgenommen wird.

Die erfindungsgemäße Lösung verhindert also nicht, daß die Postregister einschließlich Inhalt entfernt werden, um beliebig viele Kopien anzufertigen, sondern sie verhindert, daß mit Hilfe dieser Kopien Postgüter frankiert werden können, ohne daß eine adäquate Abrechnung bei der Datenzentrale bzw. Bezahlung bei der Post vorgenommen wird. Eine Verkapselung der Bauelemente für die herausnehmbaren die Postregister speichernden NV-RAMs mit einem Sicherheitsgehäuse oder das Vorsehen anderer zusätzlicher Maßnahmen zum Schutz vor Entnahme, wie Aufkleben auf die Leiterplatte, Versiegeln oder Vergießen mit Epoxidharz sind nun nicht erforderlich.

Die frankiermaschineninterne Sicherheitsschaltung für Postregisterdaten und andere sicherheitsrelevante Daten beruht auf nichtflüchtigen Speicherbausteinen. Bei der ausgeschalteten Frankiermaschine bzw. bei ausgefallener Stromversorgung bleiben die Daten gespeichert. Solche beispielsweise mit einer Lithiumbatterie gestützten CMOS-SRAM's sind während ihrer Lebensdauer von ca. 10 Jahren beliebig oft beschreibbar. Die Batterie kann weder nachgeladen noch entladen werden, ohne den Speicherbaustein zu zerstören. Es wird davon ausgegangen, daß im Leben einer Frankiermaschine bis zu 150 000 Abdrucke möglich sind und daß die Lithiumbatterie während dieser Zeit nicht ausgewechselt werden muß.

Ebenfalls können Speichermittel von anderer Speichertechnologie durch die Sicherheitsschaltung entsprechend vor Mißbrauch geschützt werden, wenn zu vorbestimmten Ereignissen sicherheitsrelevante Daten in diese nichtflüchtigen Speicher gespeichert werden.

Vom Herstellerwerk der Frankiermaschine wird in die nichtflüchtigen Speicherbausteine (Bat-NV-CMOS-SRAM's und E²PROM) ein Codewort eingespeichert, welches einer vorbestimmten Frankiermaschine zugeordnet ist. Das Codewort kann am Anfang beispielsweise

se die Seriennummer der Frankiermaschine umfassen oder kann ein Teil einer anderen Nummer sein. Außerdem werden die Registerspeicherplätze mit Anfangswerten vom Herstellerwerk vorbesetzt.

Die erfindungsgemäße Lösung gestattet festzustellen, das die nichtflüchtigen Speicher (NV-RAMs, E²PROMs) ausgewechselt und geklont wurden, um später mit den geklonten oder ausgewechselten NV-RAMs bzw. E²PROMs die Frankiermaschine FM zu betreiben. Die Erfindung geht von einem OTP-Prozessor mit einem internen OPT-ROM und internen OTP-RAM aus. Im internen OPT-ROM ist eine Liste von Codewörtern gespeichert, wobei jedes Codewort zeitweise und möglichst nur einmal aktiv ist. Das Codewort wird unabhängig vom Speicherinhalt der NV-RAMs aus der Tabelle — die im von außen nicht zugänglichen internen ROM-Bereich des OTP gespeichert vorliegt — ausgewählt.

Das neue Codewort wird mindestens beim Einschalten der Frankiermaschine der internen OTP-Tabelle entnommen und in den nichtflüchtigen Speichern (NV-RAMs, E²PROMs) abgespeichert, wenn das alte in der Liste das jeweilige Vorgänger-Codewort war.

Das Weiterschalten der Codewörter wird über Flags oder Zeiger, die in einem weiteren nichtflüchtigen Speicher gespeichert sind, realisiert. Der Zeiger wird außerhalb des zu jeweils überprüfenden nichtflüchtigen Speichers (NV-RAMs) in einem ständig eingebauten und/oder während der Laufzeit der Frankiermaschine mit ihrem Prozessorsystem in Kommunikationsverbindung stehenden und gegen Herausnahme während der Laufzeit der Frankiermaschine abgesicherten Sicherheits-Speicher gespeichert. Zur Verhinderung von Manipulationen in Fälschungsabsicht des vorgenannten ständig eingebauten und gegen Herausnahme abgesicherten Sicherheits-Speicher sollten diese Flag oder Zeiger MAC-gesichert gespeichert sein.

Das Verfahren zur Erhöhung der Manipulationssicherheit von kritischen Registerdaten umfaßt in einer weiteren Variante die folgenden Schritte:

- Laden einer Zahl oder eines Zeigers, welcher einem Codewort zugeordnet ist, in einen ersten nichtflüchtigen Speicher 20,
- Laden eines Codewortes in zweite die Postregisterdaten enthaltenden nichtflüchtigen Speicher (NVM 5a, 5b), wobei das Codewort dem letzten Betriebszustand der Frankiermaschine zugeordnet ist, d. h. das dem Ergebnis der Herstellung oder einer Nachladung der Frankiermaschine bzw. vor dem Ausschalten bzw. vor Spannungsausfall oder vor einer Stillstandszeit (Stand by) bzw. vor Programmunterbrechung entsprechend ausgewählt worden ist,
- Gültigkeitsprüfung des Codewortes mindestens zum Zeitpunkt des Einschaltens der Frankiermaschine und
- Ersetzen des alten Codewortes durch ein vorbestimmtes neues Codewort, wenn der Prozessor, nach Gültigkeitsprüfung mit Bezug auf das in seinem internen Prozessorspeicher (NVM 6c) aus einer Liste mit gespeicherten Codewörtern entsprechend der Zahl bzw. der Zeigerstellung ausgewählte Codewort, die Gültigkeit des alten Codewortes erkennt oder
- Blockierung der Frankiermaschine nach dem Zeitpunkt des Einschaltens der Frankiermaschine, wenn der Prozessor nach Gültigkeitsprüfung mit Bezug auf das ausgewählte in vorgenannter Liste

gespeicherte Codewort die Gültigkeit des alten Codewortes aberkennt.

Das Programm für die Auswahl des jeweils neuen Codewortes ist im internen Programmspeicher (internen OTP-ROM bzw. OTP-EPROM) gespeichert. Die Auswahl des neuen Codewortes ist vom vorherigen und/oder vom Zustand der Frankiermaschine zu einem vorbestimmten Zeitpunkt abhängig. Jedem nichtflüchtigen Speicher oder Speicherbereich, der geschützt werden muß, kann ein separates Codewort zugeordnet werden.

Es ist vorgesehen, daß in einem Schritt zur Bildung eines neuen veränderbaren ersten Codewortes auch die Bildung des neuen zweiten Codewortes nach einem identischen Algorithmus zur Bildung des neuen ersten Codewortes erfolgt, um ein identisches neues zweites Codewort in die zu schützenden nichtflüchtigen Speicher zu laden.

Alternativ ist in einer weiteren Variante vorgesehen, daß in einem Schritt zur Bildung eines neuen veränderbaren ersten Codewortes auch die Bildung des neuen zweiten Codewortes als komplementärer Schatten zum neuen ersten Codewortes erfolgt, um ein komplementäres neues zweites Codewort in die zu schützenden nichtflüchtigen Speicher zu laden.

Es ist in einer anderen Variante vorgesehen, daß in einem Schritt zur Bildung eines neuen veränderbaren ersten Codewortes auch die Bildung des neuen zweiten Codewortes als zu dem veränderbaren neuen ersten Codewort identischen Codewort und als komplementärer Schatten zum neuen ersten Codewortes erfolgt, um mindestens ein neues zweites Codewort in die zu schützenden nichtflüchtigen Speicher zu laden oder daß beim Schutz eines entsprechenden Speichers in mindestens einem der Speicherbereiche auch mit dem komplementären Schatten gearbeitet wird.

Für eine Anordnung zur Erhöhung der Manipulationssicherheit von kritischen Daten, insbesondere von Registerdaten in Frankiermaschinen mit einer Steuereinrichtung und Speichern, ist vorgesehen, daß die Steuereinrichtung einen Mikroprozessor oder einen OTP-Prozessor (ONE TIME PROGRAMMABLE) aufweist und im OTP sind neben einem Mikroprozessor CPU auch weitere Schaltungen und/oder Programme bzw. Daten im internen OTP-ROM bzw. im internen OTP-RAM in einem gemeinsamen Bauelementgehäuse untergebracht sind, welche ein erstes Sicherheitsmittel gegen unbefugte Manipulation bilden sowie daß ein externer nichtflüchtiger Speicher NVM 20 ein zweites Sicherheitsmittel gegen unbefugte Manipulation bildet.

Vorteilhafte Weiterbildungen der Erfindung sind in den Unteransprüchen gekennzeichnet bzw. werden nachstehend zusammen mit der Beschreibung der bevorzugten Ausführung der Erfindung anhand der Figuren näher dargestellt. Es zeigen:

Fig. 1, Blockschaltbild einer Frankiermaschine mit erfindungsgemäß erhöhter Sicherheit,

Fig. 2, Variante mit OTP-Prozessor,

Fig. 3, Gesamtablaufplan für die Frankiermaschine,

Fig. 4, Details des Ablaufplans nach Fig. 3,

Fig. 5, Ablaufplan für den Frankiermodus,

Fig. 6, Details des Ablaufplans nach Fig. 4,

Fig. 7, Flußplan für das erfindungsgemäße Verfahren zur Erhöhung der Manipulationssicherheit,

Fig. 8a bis c, Zeigerstellungen nach dem erfindungsgemäßen Verfahren.

Die Fig. 1 zeigt ein Blockschaltbild der erfindungsge-

mäßen Frankiermaschine mit einem Druckermodul 1 für ein vollelektronisch erzeugtes Frankierbild, mit mindestens einem mehrere Betätigungselemente aufweisenden Eingabemittel 2, einer Anzeigeeinheit 3, einem die Kommunikation mit einer Datenzentrale herstellenden MODEM 23, welche über einen Ein/Ausgabe-Steuermodule 4 mit einer Steuereinrichtung 6 gekoppelt sind und mit mindestens einem nichtflüchtigen Speicher 5a bzw. 5b für die variablen und einen Speicher 10, 11 für die konstanten Teile des Frankierbildes.

Ein Charakterspeicher 9 liefert die nötigen Druckdaten für einen flüchtigen Arbeitsspeicher 7. Der flüchtige Arbeitsspeicher 7 umfaßt beispielsweise einen externen RAM in Verbindung mit einem im Prozessor angeordneten internen RAM 6b. Die Steuereinrichtung 6 weist einen entsprechend ausgebildeten Mikroprozessor μP auf und ist mit dem Ein/Ausgabe-Steuermodule 4, dem Charakterspeicher 9, dem flüchtigen Arbeitsspeicher 7, mit einem nichtflüchtigen Kostenstellenspeicher NVM 5a und mit einem nichtflüchtigen Arbeitsspeicher NVM 5b, mit einem anwendungsspezifischen Programmspeicher ASP 10 (Klischee-EPROM), einem Programmspeicher PSP 11 (Programm-EPROM), mit dem Motor einer Transport- bzw. Vorschubvorrichtung ggf. mit Streifenauflösung 12, einem Encoder (Codierscheibe) 13, einem Brieftensor 16 sowie mit einem Uhren/Datums-Baustein 8 verbunden. Ein entsprechendes Verfahren zum Steuern eines spaltenweisen Drucks eines Postwertzeichenbildes ist beispielsweise in der EP 578 042 A2 oder in der EP 576 133 A2 ausführlicher beschrieben.

Die — in der Fig. 2 näher dargestellte — Steuereinrichtung 6 weist einen Mikroprozessor oder einen OTP-Prozessor (ONE TIME PROGRAMMABLE) auf. Im OTP sind neben einem Mikroprozessor CPU 6a auch weitere Schaltungen in einem gemeinsamen Bauelementgehäuse untergebracht. Diese weiteren Schaltungen und/oder Programme bzw. Daten im internen OTP-ROM 6c bzw. im internen OTP-RAM 6b in dem gemeinsamen Prozessorgehäuse bilden eine Sicherheitsschaltung bzw. ein erstes Sicherheitsmittel gegen unbefugte Manipulation.

Die übrigen einzelnen Speicher können in mehreren physikalisch getrennten oder in gemäß der Fig. 2 gezeigten Weise in wenigen Bausteinen zusammengefaßt verwirklicht sein. Vorzugsweise sind die Festwertspeicher CSP 9 und PSP 11 in einem EPROM und die nichtflüchtigen Speicher NVM 5a und 5b in einem Postregisterspeicher zusammengefaßt. Letzterer ist vorzugsweise doppelt vorhanden und wird in seinen Speicherbereichen redundant mit Daten beschrieben. Ein Verfahren zum Speichern sicherheitsrelevanter Daten ist beispielsweise in der EP 615 211 A1 näher ausgeführt.

Ein externer nichtflüchtiger Speicher NVM 20 bildet ein zweites Sicherheitsmittel gegen unbefugte Manipulation. In der Fig. 1 wird ein Blockschaltbild der erfindungsgemäßen Frankiermaschine 1 mit einer Chipkarten-Schreib-Lese-Einheit 21 dargestellt. Diese steht über einen BUS 11 mit einem Prozessor 6 direkt oder über Ein/Ausgangsmittel (I/O-Ports) 4 in Verbindung. Weiter ist ein — in der Fig. 1 nicht näher dargestellter — Anschluß eines MODEMs 23 über den BUS 11 direkt oder über vorgenanntes Ein/Ausgangsmittel 4 vorgesehen. Sowohl in der Datenzentrale als auch in einer Chipkarte, welche in die Chipkarten-Schreib-Lese-Einheit 21 eingesteckt werden muß, schließen einen externen nichtflüchtigen Speicher ein, welcher als zweites Sicherheitsmittel gegen unbefugte Manipulation, eingesetzt werden kann.

Der externe nichtflüchtige Speicher NVM 20 ist in der bevorzugten Variante — wie in der Fig. 1 gezeigt — ein Bestandteil des Prozessorsystems der Frankiermaschine und arbeitet mit dem Programmspeicher 6c (internes EPROM oder ROM) und flüchtige Datenspeicher RAM 6b zusammen.

Durch die Möglichkeit Sicherungsbits zu setzen, (bei internen EPROM) bzw. während der Herstellung eine Maskenprogrammierung (bei internen ROM) vorzunehmen, kann das Auslesen des internen Programmspeichers von außen verhindert werden. Die Sicherungsbits werden durch Programmierung des internen EPROM während der Herstellung der Frankiermaschine im OTP-Prozessor gesetzt. Das Observieren solcher sicherheitsrelevanter Routinen, wie beispielsweise Abrechnungsroutinen, mit einem Emulator/Debugger würde ebenfalls zu einem veränderten Zeitablauf führen, was durch den OTP feststellbar ist. Dieser umfaßt auch eine Taktgeber/Zähler-Schaltung für die Vorgabe von Zeitintervallen bzw. Taktzyklen beispielsweise für die Time-out-Generierung oder Druckersteuerung. Vorteilhaft wird die Taktgeber/Zähler-Schaltung für eine Programmlaufzeitüberwachung eingesetzt, welche in der Anmeldung EP 660 269 A2 genauer beschrieben ist. Wenn eine bestimmte Zeit abgelaufen und das erwartete Ereignis nicht eingetreten ist, wird vom der Taktgeber/Zähler-Schaltung ein Interrupt generiert, der dem Mikroprozessor den ergebnislosen Ablauf der Zeitspanne meldet, woraufhin der Mikroprozessor weitere Maßnahmen veranlaßt. Die Überwachungsfunktion wird in vorgenannter Weise durch das vorgenannte erste Sicherungsmittel übernommen, das Bestandteil des Prozessors (OTP) ist und die in Verbindung mit einer entsprechenden Software während des Betriebes der Frankiermaschine wirksam wird. Bei einer vorteilhaften weiteren Variante der Zeitkontrolle wird ein Codewort im externen NVM 5a, 5b oder 20 gelöscht. Das kann durch Überschreiben mit einem vorbestimmten anderen Wort, beispielsweise 0000 erfolgen. Der Vorteil liegt insbesondere darin, daß die Sicherheitsschaltung während des Betriebes auf eine Manipulation durch unbefugten Eingriff in die Frankiermaschine reagiert.

Die frankiermaschineninterne Sicherheitsschaltung für Postregisterdaten und andere sicherheitsrelevante Daten schützt den Dateninhalt von nichtflüchtigen Speichern, beispielsweise von mit einer Lithiumbatterie gestützten CMOS-SRAM's, gegenüber einer Verwendung unerlaubt geklonter Kopien ohne Abrechnung.

Vorgenannte Lithiumbatterie gestützten CMOS-SRAM's haben eine Lebensdauer von mindestens 10 Jahren. Als nichtflüchtige Speicherbausteine sind beispielsweise von Dallas Semiconductor beim Typ DS1230Y/AB ein Speicherbereich von 256 K oder ein Speicherbereich von 1024 K für ein NV-SRAM beim Typ DS1245Y/AB verfügbar.

Ebenfalls kann der Uhren/Datums-Baustein 8 nach dem gleichen Verfahren geschützt werden. Dieser vorgenannte Baustein ist ein nichtflüchtiger Zeitgeber-RAM und enthält ebenfalls eine Lithiumbatterie für mindestens 10 Jahre. Der Baustein DS 1642 von Dallas Semiconductor weist einen $2K \times 8$ NV-SRAM auf.

Zusätzlich sind auch Speichermittel von anderer Speichertechnologie entsprechend ihrer Lebensdauer einsetzbar. Die Sicherheitsschaltung speichert in diese nichtflüchtigen Speicher beispielsweise nur Daten zum Zeitpunkt des Einschaltens bzw. Wiederinbetriebnahme der Frankiermaschine nach einem Stand by-Betrieb, also zu Zeitpunkten, wo kein Abrechnungserfordernis

vorliegt und keine Frankierung erfolgt. Normale EPROM-Speicher, insbesondere vom Typ 28256 benötigen keine interne Batterie und lassen mindestens 10 000 bis 100 000 Schreib-/Lese-Zyklen zu. Die frankiermaschineninterne Sicherheitsschaltung für Postregisterdaten und andere sicherheitsrelevante Daten steuert entsprechend die vorgenannten nichtflüchtigen Speicherbausteine so an, daß die Lebensdauer erhöht bzw. ausreichend ist.

Wenn in den nichtflüchtigen Speichern 5a, 5b neben einem Codewort der Dateninhalt der Postregister als Checksumme verschlüsselt gespeichert wird, kann die Manipulation der Postregister wirksam von Anfang an verhindert werden. Beispielsweise wird ein OTP-Prozessor (ONE TIME PROGRAMMABLE) eingesetzt, der im internen ROM einen gespeicherten Algorithmus für ein solches Prüfsummenverfahren aufweist. Gesetzte Flags verhindern ein Auslesen der sicherheitsrelevanten Daten aus dem Prozessor. Ein bekanntes Prüfsummenverfahren beruht auf einem MAC (MESSAGE AUTHENTICATION CODE) der an die zu sichernden Daten angehängt wird. Eine solche MAC-Absicherung wird vorteilhaft über die Postregisterdaten gelegt. Im Regelfall genügt jedoch ein Codewort, welches in Zeitabständen geändert wird, um die Sicherheit zu garantieren.

Als Prozessor kann beispielsweise ein 8051-Prozessor mit einem 16 kByte On-Chip-EPROM als internen Programmspeicher eingesetzt werden. Der interne OTP-RAM hat einen Speicherbereich von 256 Byte.

Erfindungsgemäß ist nun vorgesehen, daß die die Postregisterdaten enthaltenen nichtflüchtigen Speicher, insbesondere batteriegestützte CMOS-RAM's (Bat-NV-CMOS-RAM's) ein Codewort enthalten, welches dem letzten Betriebszustand der Frankiermaschine vor dem Ausschalten bzw. Spannungsausfall oder vor einer gewissen Stillstandszeit (Stand by) bzw. vor Programmunterbrechung entsprechend gewählt wurde und daß mindestens zum Zeitpunkt des Einschaltens der Frankiermaschine das alte Codewort durch ein vorbestimmtes neues Codewort ersetzt wird.

Erfindungsgemäß wird also das Codewort zu vorbestimmten Ereignissen durch die betriebsbereite Frankiermaschine automatisch in allen nichtflüchtigen Speichern, welche sicherheitsrelevante Daten handeln, geändert. Eine derartige Maßnahme verhindert, daß ein geklonter Speicherinhalt eines nichtflüchtigen Speichers (Bat-NV-CMOS-RAM's) öfter als einmal verwendet werden kann, weil, das Codewort im nichtflüchtigen internen Prozessorspeicher und im Postregister (Bat-NV-CMOS-RAM's) geändert wird, sobald ein vorbestimmter Betriebszustand der Frankiermaschine nach dem Einschalten der Maschine bzw. nach Spannungswiederkehr nach einem Ausfall, nach Verlassen des Kommunikationsmodus bzw. dem Nachladen der Frankiermaschine mit einem Guthaben oder nach einer gewissen Stillstandszeit (Stand by) erreicht ist oder nach einer anderen Programmunterbrechung.

Dabei wird durch o.g. Maßnahme ein Duplizieren bzw. Klonen eines Bat-NV-CMOS-RAM's oder anderen NVRAM's nicht verhindert. Auch ein Duplikat des Speicherinhalts, welches gegen den Speicherinhalt des Originals ausgetauscht wird, kann weiterverwendet werden. In diesem Fall wird das Codewort des Originals später ungültig, d. h. ein Rücktausch der Speicherinhalte würde vom Prozessor aufgrund des inzwischen ebenfalls geänderten Codewortes im nichtflüchtigen internen Prozessorspeicher bemerkt werden.

Die Veränderung der Codeworte bei gleichgebliebenen Dateninhalt des Speichers kann ohne Kenntnis des Schlüssels und der Parameterdaten vom Manipulator auch nicht vorgenommen werden, wenn der Algorithmus zur Bildung des neuen Codewortes bekannt wäre. Deshalb kann ein bekanntes Verschlüsselungsverfahren, wie beispielsweise DES, eingesetzt werden.

Das Verfahren zur Erhöhung der Manipulationssicherheit von kritischen Registerdaten umfaßt weitere Sicherungsschritte, die in der Fig. 7 dargestellt sind.

Im Schritt 106 werden nacheinander die in den zu schützenden nichtflüchtigen Speichern gespeicherten Codewörter gelesen und dann zum Prozessor übertragen. Der Prozessor führt einen Sicherungsschritt 107 zur Überprüfung des bisher gültigen Codewortes und einen Schritt 108 zur entsprechenden Veränderung des Codewortes aus, wenn die Überprüfung die Übereinstimmung bzw. Fehlerfreiheit ergeben hat. Anderenfalls wird vom Schritt 107 auf den Schritt 109 verzweigt, um einen eine den Kill-Mode kennzeichnende Zahl bzw. mindestens aber ein MAC-gesichertes Kill-Mode-Flag im ständig eingebauten nichtflüchtigen externen Sicherheits-Speicher zu setzen.

In den Fig. 8a bis c werden Zeigerstellungen nach dem erfindungsgemäßen Verfahren dargestellt. Die Fig. 8a zeigt eine Anfangszustandsvoreinstellung. Eine solche wird im Schritt 107 (Fig. 7) benötigt, um das richtige alte Codewort aus der gespeicherten Liste zu ermitteln. Der Zeiger steht beim ersten Initialisieren der Maschine im Herstellerwerk auf einer Zahl 1. Alternativ kann auch die Seriennummer der Frankiermaschine eine Anfangszahl bilden. Die Zeigerstellung (Zahl 1 bzw. Anfangszahl) wird gespeichert. Dann wird ein entsprechender erster Code, der in der Liste an einer ersten Stelle steht im zu schützenden NVM 5a bzw. 5b gespeichert. Die Frankiermaschine verläßt das Herstellerwerk auf eine Zahl 1 bzw. Anfangszahl gestellt. Beim Händler bzw. beim Kunden wird nun die Frankiermaschine eingeschaltet bzw. wiedereingeschaltet (Fig. 8b). Der erste Code wird entsprechend der Zeigerstellung aus der Liste gelesen und mit dem im zu schützenden NVM 5a bzw. 5b gespeichert vorliegenden ersten Code verglichen. Diese erste Phase entspricht dem Schritt 107 der Fig. 7, in welcher festgestellt wird ob ein Speicher zwischenzeitlich ohne abzurechnen herausgenommen und durch einen anderen ersetzt worden war und nun erneut mit alten Datenbestand eingesetzt wurde. Sind die Code gleich, wird entsprechend der Fig. 8c die Zeigerstellung auf ein zweites Codewort in der Liste weitergeschaltet, was dem Schritt 108 in der Fig. 7 entnehmbar ist. Die Zeigerstellung wird in vorbestimmter Weise verändert. Im einfachsten Fall wird die Zeigerstellung inkrementiert oder dekrementiert.

Der erste Code im zu schützenden NVM 5a bzw. 5b wird nun durch den zweiten Code ausgetauscht, d. h. überschrieben. Wird nun nach dem Ausschalten die Frankiermaschine eingeschaltet bzw. wiedereingeschaltet wird eine Überprüfung auf der Basis des aktuellen Code analog zu der Fig. 8b und Fig. 7, Schritt 107 gezeigten Weise vorgenommen.

Im bevorzugten Ausführungsbeispiel wird für zwei nichtflüchtige Speicher NVM 6d und NVM 5a im Schritt 107 zur Überprüfung des bisher gültigen Codewortes V(-1), U(-1) ein für jeden physikalischen Speicherbaustein vorgesehenes separates Codewort W(-1), T(-1) verwendet.

Für zwei nichtflüchtige Speicher NVM 20 und NVM 5a wird nach Überprüfung des alten Codewortes im

Schritt 107 und vor der entsprechenden Veränderung von Codewörtern V und U zunächst im Schritt 108 ein neues Codewort W' und danach ein Codewort T' gebildet, nach den Gleichungen:

$$W' := F\{P1\} \text{ und } (1)$$

$$T' := F\{P2\}, \quad (2)$$

wobei P1 und P2 gelistete Codewörter sind.

In einer Variante werden mit den gelisteten Codewörtern und mit internen Daten nach einem internen Programm ein neues Codewort mittels einer solchen mathematischen Funktion F erzeugt, welche das externe Nachbilden von Codewörtern wesentlich erschwert, so daß eine Manipulation in Fälschungsabsicht praktisch unmöglich gemacht wird.

Im einfachsten Fall wird im internen NVM 20 ein Zählwert inkrementiert, bevor ein neues Codewort (W', T', U', V') gebildet wird. Als mathematische Funktion F kann beispielsweise eine kryptographische Funktion verwendet werden, welche im internen OTP-ROM als Algorithmus bzw. Programm gespeichert vorliegt. Zum Beispiel kann der DES-Algorithmus (Data-Encryption-Standard) oder eine Zufallsfunktion eingesetzt werden, beispielsweise um den neuen Zeiger entsprechend F zu ermitteln.

Das vorgenannte Bilden von Codewörtern umfaßt das Berechnen und/oder das Auswählen aus einer Liste von Codewörtern, welche im internen OTP-ROM gespeichert vorliegt. Im Idealfall soll jedes Codewort nur ein einziges mal zur Absicherung der externen nichtflüchtigen Schreib/Lese-Speicher verwendet werden. Das erfordert aber eine Vielzahl von Codewörtern, welche im internen OTP-ROM gespeichert werden.

Lediglich die Zeigerstellung oder Zahl die auf die Stellung des jeweiligen Codewortes in der in OTP-ROM gespeicherten Liste hinweist muß extern vom OTP-Prozessor und extern von den zu schützenden nichtflüchtigen Schreib/Lese-Speichern NVM 5a und 5b besonders gesichert gespeichert werden. Dieses Sichern des zweiten Sicherheitsmittels 20 gegen Entnahme aus dem Prozessorsystem kann durch ein Aufkleben oder ein gesichertes Kapseln des vorgenannten Sicherheits-Speichers zusammen mit dem Prozessor gewährleistet werden.

Bei den erfindungsgemäßen Varianten mit Speicherung in der Datenzentrale oder Chipkarte kann auf ein Aufkleben oder ein gesichertes Kapseln mindestens eines der externen nichtflüchtigen Schreib/Lese-Speicher verzichtet werden.

Diesen Varianten liegt die Voraussetzung zugrunde, daß der Speicher der Datenzentrale bzw. der Chipkarte nicht manipuliert oder geklont werden kann. Ein Manipulator darf das neu zu bildende Codewort vor dem Einschalten nicht abfragen können, um damit seine geklonten Speicher auszurüsten. Die Zeigerstellung bzw. Zahl kann mittels DES verschlüsselt werden, wenn diese zur Datenzentrale übermittelt bzw. zur Chipkarte transferiert wird. Alternativ wird das Codewort übermittelt, oder nur die Anweisung zu seiner Wiederherstellung oder wesentliche Teile der Anweisung. Die Übermittlung erfolgt wieder verschlüsselt bzw. MAC-gesichert. Ein solches Verfahren hat den Vorteil, daß man ohne o.g. speziellen Prozessor auskommt und daß dennoch alle Postregister-NVRAMs weiterhin gesockelt und somit leicht austauschbar montiert sind.

Alternativ ist es auch möglich, daß ein in der Liste gespeichertes Codewort verschlüsselt ausgelesen wer-

den kann, wenn ein spezieller Prozessor vorliegt. Die Codewörter aus dem zu schützenden Speicher und das Codewort aus der vorgenannten Liste, auf welches der Zeiger weist, werden verschlüsselt zur Datenzentrale übermittelt bzw. zur Chipkarte übertragen, wobei letztere den Vergleich zwecks Sicherheitsüberprüfung vornehmen.

In einer weiteren Variante wird von der Frankiermaschine das Codewort zum Speicher der Datenzentrale übertragen. Bei jedem Einschalten der Frankiermaschine wird eine Verbindung zur Datenzentrale hergestellt. Die Fehlerfreiheit wird durch Vergleich des extern in der Datenzentrale gespeicherten Codewortes mit dem in den Postregister-NVRAM gespeicherten Codewort festgestellt, um dann ein neues Codewort zu bilden und im NVRAM der Datenzentrale und im Postregister-NVRAM abzuspeichern. Der Vergleich kann in der Datenzentrale oder in der FM durchgeführt werden. Eine Alternative besteht im Abspeichern des Codewortes in einem speziellen Übertragungsmittel (z. B. Chipkarte). Eine Telefonverbindung zur Datenzentrale wäre dann keine Voraussetzung zur Inbetriebnahme der Frankiermaschine, wenn zu Beginn die Chipkarte gesteckt wurde. Es ist ein entsprechender Kommunikations-Modus 300 nach dem Einschalten während der Laufzeit der Frankiermaschine vorgesehen.

Das erfindungsgemäße Verfahren ist in einem — in der Fig. 3 dargestellten — Gesamtablaufplan der Frankiermaschine eingebunden. Nach dem Start 100 erfolgen in einem die Startroutine und Initialisierung umfassenden Schritt 101 Maßnahmen zur Sicherheitsüberprüfung und zur Wiederherstellung eines definierten Anfangszustandes.

Die weiteren Schritte 102 bis 105 erfolgen gegebenenfalls zur Wiederherstellung der Betriebsbereitschaft beispielsweise nach einer Reparatur der Frankiermaschine und sind in der Fig. 7 näher dargestellt.

In den Schritten 106 bis 109 werden die gelesenen alten Codewörter überprüft und gegen neue Codewörter ausgetauscht. Anschließend wird das neue Codewort auch in die NV-RAMs NVM 5a und NVM 5b übertragen und bildet dort ein entsprechendes Codewort (V', U'). Der Schritt 108 beinhaltet außerdem die Überprüfung des ordnungsgemäßen Einspeicherns der Codewörter (U', V' bzw. W', T'). Wird bei der Überprüfung des bisher gültigen Codewortes eine nicht plausible Abweichung festgestellt, wird zu einem Schritt 109 verzweigt, der Maßnahmen umfaßt, die letztlich weitere Frankierungen für die Frankiermaschine verhindern. Beispielsweise kann ein drittes von einer Datenzentrale vorgegebenes Codewort Y gelöscht werden, dessen Fehlen die Manipulation belegt. Nachfolgend wird auf die Systemroutine (Punkt s) verzweigt.

Der in der Fig. 3 dargestellte Gesamtablaufplan für die Frankiermaschine weist Schritte 201 bis 206 und 207 bis 208 für eine Überwachung weiterer Kriterien auf. Bei einer Verletzung beispielsweise eines im Schritt 207 überprüften Sicherheitskriteriums tritt die Frankiermaschine in einen entsprechenden Kill-Modus ein (Schritt 208). Die Frankiermaschine tritt aufgrund eines im Schritt 202 überprüften Sicherheitskriteriums in einen Sleeping-(Warn)-Modus (203—206) ein, wenn nach Verbrauch einer vorbestimmten Stückzahl noch keine Verbindung zur Datenzentrale aufgenommen wurde.

Die Frankiermaschine und die Datenzentrale verabreden jeweils eine vorbestimmte Stückzahl S, d. h. die Menge, die bis zur nächsten Verbindungsaufnahme frankiert werden kann. Falls eine Kommunikation nicht

zustande kommt (Stückzahlkontrolle), verlangsamt die Frankiermaschine ihre Arbeitsweise (Sleeping Modus-Variante 1), damit bis zu einer nächsten Stückzahlgrenze ohne Anzeige einer Warnung weiter gearbeitet werden kann. Jedoch ist es möglich in immer kürzeren Abständen, d. h. nach einer vorbestimmten Anzahl an Frankierungen, eine erneute Warnung auszugeben, welche so immer dringlicher auf das Erfordernis einer Kommunikation mit der Datenzentrale aufmerksam macht (Sleeping Modus-Variante 2). Schließlich ist es möglich (Sleeping Modus-Variante 3), eine ständige Warnung für ein bevorstehendes Schlafenlegen der Frankierfunktion im Schritt 203 auszugeben, wenn dieser aufgrund des erfüllten Abfragekriteriums in Schritt 202 ständig durchlaufen werden muß, bevor Schritt 205 erreicht wird. Es ist weiterhin vorgesehen, daß der Schritt 203 einen Subschritt zur Fehlerstatistik entsprechend dem Statistik- und Fehlerauswertungsmodus 213 umfaßt. Diese Variante kommt ohne den vorgenannten Schritt 204 aus. Das Frankieren wird durch den Sleeping Modus nicht beeinträchtigt. Solange die Überprüfung im Schritt 205 ergibt, daß die Stückzahl S noch größer Null ist, wird der Schritt 207 erreicht. Lediglich die Warnung erscheint immer öfter in der Anzeige. Anderenfalls wird auf den Schritt 206 verzweigt, wobei beispielsweise ein FLAG gesetzt wird, welches später im Schritt 301 abgefragt und als Kommunikationsersuchen gewertet wird. Im Schritt 206 kann ebenfalls eine zusätzliche Anzeige erfolgen, daß nun automatisch die Kommunikation erfolgt und solange die Frankierfunktion ruht, bis die Kommunikation erfolgreich abgeschlossen ist. Natürlich kann jederzeit der Frankiermaschinenbenutzer schon vorher den Kommunikationsmodus 300 aufrufen. In einem dem Kommunikationsmodus 300 vorausgehenden Schritt 207 werden weitere für die Manipulationssicherheit relevante Kriterien überprüft. Bei einer festgestellten Manipulation der Maschine, die in Fälschungsabsicht vorgenommen wurde, wird zum Schritt 208 verzweigt, um ein Frankieren mit der manipulierten Maschine zu verhindern. Die Maschine würde in einem solchen Fall in den Kill-Mode eintreten. Befindet sich die Frankiermaschine nur im Sleeping-Mode wird ein Frankieren nicht verhindert.

Nach der Überprüfung der Kriterien für den Kill-Modus (Schritte 207 bis 208) und für den Sleeping-Modus (Schritte 202 bis 206) wird ein in der Fig. 3 gezeigter Punkt t erreicht. Im Schritt 209 können Eingaben getätigt werden, bevor der Punkt e erreicht wird.

Mit dem Eintritt in den Kommunikationsmodus 300 besteht für den Nutzer die Möglichkeit eine Kommunikation mit der Datenzentrale herbeizuführen bzw. es wird gegebenenfalls eine Kommunikation mit der Datenzentrale automatisch — gemäß dem in der Fig. 3 gezeigten Gesamtablaufplan — herbeigeführt.

Falls die Kommunikation erfolgreich war, wird im Schritt 211 abgefragt, ob Daten übermittelt wurden. Anschließend wird der Schritt 213 erreicht. Im Schritt 213 werden die aktuellen Daten ermittelt bzw. geladen, welche im Schritt 201 aufgerufen und anschließend wieder beim Vergleich im Schritt 202 benötigt werden.

Das übermittelte Entscheidungskriterium ist vorzugsweise die neue Stückzahl S'.

Der Auswertemodus im Schritt 213 umfaßt erfindungsgemäß auch die Bildung neuer Codewörter U', V' für die zu schützenden nichtflüchtigen Speicher im Ergebnis eines Nachladevorganges, der in Kommunikationsverbindung mit einer Datenzentrale vorgenommen wurde. Hierbei laufen die in der Fig. 7 für Codewort Y

beispielhaft gezeigten Schritte 106 bis 109 in analoger Weise auch für die Codewörter U', V' ab.

Wurde zuvor bei der Datenzentrale eine Eingriffsbefugnis für die Frankiermaschine angefordert, wird ein von der Datenzentrale vorgegebenes neues drittes Codewort Y' geladen, welches das alte dritte Codewort Y ersetzen kann. Für Reparaturzwecke ist ein Öffnen der Frankiermaschine und ein Austausch defekter Bauelemente ggf. unvermeidlich. Deshalb sind vorausgehende Maßnahmen zur Erlangung einer Eingriffsbefugnis erforderlich, welche den Betrieb der Frankiermaschine nach deren Instandsetzung erlauben. Ein unbefugtes Öffnen der Frankiermaschine wird dabei ausgeschlossen. Wenn die Frankiermaschine nach dem Eingriff wieder in Betrieb genommen wird, kann aufgrund der Eingriffsbefugnis für die Frankiermaschine jenes von einer Datenzentrale vorgegebenes neues dritte Codewort Y' das alte dritte Codewort Y ersetzen, wie dies beispielsweise in der Anmeldung DE 43 44 476 A1 vorgeschlagen wurde.

Sollte also das von einer Datenzentrale vorgegebene alte dritte Codewort y gelöscht werden, weil die Speicher vollständig ausgetauscht wurden und deren veränderbares Codewort (V, U) nicht vorhanden ist, bzw. nicht mit dem intern gespeicherten übereinstimmt, würde die Frankiermaschine weiterbetrieben werden können.

Der Weiterbetrieb der Frankiermaschine ist möglich, weil ein neues drittes Codewort Y' verwendet wird, wobei — wie in der Fig. 7 dargestellt ist — auf den Schritt 108 verzweigt wird, um ein neues veränderbares Codewort (T', W') zu bilden und als Codewort (V', U') in die NV-RAMs zu laden.

In einer — gegenüber dem in der Fig. 7 gezeigten Flußplan — modifizierten Flußplanvariante kann anstatt mit einem zu dem veränderbaren Codewort (W, T) identischen Codewort (V, U) auch mit dem komplementären Schatten (V'', U'') in mindestens einem der Speicherbereiche bzw. NVRAM's gearbeitet werden. Entsprechend verändern sich auch die Form der Überprüfung der bisher gültigen Codewörter und deren Ersatz durch neue Codewörter in einem der Speicherbereiche des nichtflüchtigen Speichers NVM 5a, 5b gemäß der — in den Fig. 3 und 5 gezeigten — Schritte 102 bis 105. Nach einem Verifizieren der gegebenenfalls in einem Speicherbereich E des NVM 5a, 5b gespeichert vorliegenden neuen Codewörter V', U' und/oder Y' werden die alten Codewörter gelöscht und die neuen Codewörter entsprechend abrufbar adressiert. Das kann vorteilhaft analog zum Ablauf — wie er in der Fig. 7 in DE 43 44 476 A1 dargestellt ist — erfolgen, indem die neuen Codewörter V', U' und/oder Y' auf die Adresse der alten Codewörter V, U und/oder Y gesetzt werden.

Nach einem vorausgehenden Ereignis bzw. einer Programmunterbrechung (Stand by) wird ein Punkt p erreicht und gemäß den — in der Fig. 4 dargestellten — Details des Ablaufplanes wird über Schritte 102 bis 105 ein erster Sicherungsschritt 106 des in der Fig. 7 gezeigten Flußplanes des erfindungsgemäßen Verfahrens erreicht.

Nur bei einer Inbetriebnahme oder nach Spannungsausfall wird nach einem Initialisieren in einem dem vorgenannten Punkt p vorgelagerten Schritt 1050 zuerst das aktuelle Programmmodul PM entsprechend der Modulkennung aufgerufen, dessen Abschnitte anschließend weiter bearbeitet werden sollen. Der in der Fig. 3 gezeigte Schritt 101 umfaßt mehrere Subschritte, welche nachfolgend anhand der Fig. 4 näher erläutert werden.

Zunächst laufen im Schritt 1010 übliche Hardware- und Anzeige-Initialisierungsroutinen ab, bevor ein Schritt 1011 zum Timer- und Interrupt-Start erreicht wird. Das interne Programm beginnt dann mit Startsicherheitsüberprüfungen. In vorteilhafter Weise kann hier im Schritt 1020 bereits geprüft werden, ob ein Codewort oder Speicherinhalt gültig ist. Anschließend wird bei Gültigkeit ein Schritt 1040 zur automatischen Eingabe gespeicherter Daten mit Druckdatenaufbereitung und Einbettung der Bilddaten erreicht.

Nach dem Aufruf des Merkers oder Zeigers im Schritt 1051 wird in einem weiteren Schritt 1052 getestet, ob der Programmmodul weiterabgearbeitet werden muß. Ist das nicht der Fall wird im Schritt 1054 der nächste Programmmodul PM(+1) aufgerufen. Anderenfalls wird in einem Schritt 1053 überprüft, ob Programmabschnitte eines vorhergehenden Programmmoduls PM(-1) zuende abgearbeitet werden müssen und zu einem Schritt 1056 verzweigt oder zu einem Schritt 1055 verzweigt, wenn ein Programmabschnitt des aktuellen Programmmoduls PM weiter abgearbeitet werden muß. Nach Feststellung des aktuellen Programmmoduls gemäß den Schritten 1054, 1055 oder 1056 wird auf den Punkt p verzweigt.

Für eine Abarbeitung kritischer und unkritischer Programmabschnitte innerhalb dieses Programmmoduls werden Merker, beispielsweise eine Phasenkennung gesetzt, wie das aus DE 42 17 830 A1 bekannt ist, oder Zeiger gestellt, welche nach Spannungsausfall und Wiedereinschalten eine Rekonstruktion definierter Zustände für die weitere Programmabarbeitung ermöglicht.

Gemäß der Fig. 3 wird nach Ausführung der Schritte 102 bis 105 und 106 bis 109 der Punkt s und damit die Systemroutine 200 erreicht. Außerdem wird der Punkt s nach Ausführung der Schritte für einen Testmodus 216, für einen Anzeigemodus 215 und für einen Frankiermodus 400 erreicht.

Die Erläuterung der Abläufe nach dem — in der Fig. 5 gezeigten — Frankiermodus 400 erfolgt in Verbindung mit dem — in der Fig. 1 dargestellten — Blockschaltbild und in dem — in der Fig. 3 dargestellten — Gesamtablaufplan der elektronischen Frankiermaschine.

Die Erfindung geht davon aus, daß nach dem Einschalten automatisch der Postwert im Wertabdruck entsprechend der letzten Eingabe vor dem Ausschalten der Frankiermaschine und das Datum im Tagesstempel entsprechend dem aktuellem Datum vorgegeben werden, daß für den Abdruck die variablen Daten in die festen Daten für den Rahmen und für alle unverändert bleibenden zugehörigen Daten elektronisch eingebettet werden (Fig. 4, Schritt 1040).

Außerdem läuft die Zeit im batteriegestützten Uhren/Datums-Baustein 8 ständig auch bei ausgeschalteter Frankiermaschine weiter und wird ständig aktuell mindestens als Datum gespeichert und im Schritt 1040 der Fig. 4 in der Initialisierungsroutine 101 eingebettet.

Wird also nach dem Einschalten der Frankiermaschine, nach der durchgeführten Systemroutine 200 und während des Betriebsmodus der Schritt 401 im Frankiermodus 400 erreicht, kann auch ohne Eingabe auf bereits gespeicherte Daten zurückgegriffen werden. Diese Einstellung betrifft insbesondere die letzte Einstellung der Frankiermaschine hinsichtlich des Portowertes, welche im Schritt 209 angezeigt wird, bevor ggf. eine erneute Eingabe, Anzeige und Druckdatenaufbereitung erfolgt. Hierbei werden die aktuellen variablen Pixelbilddaten (Datum und Portowert) in die festen

Rahmenpixelbilddaten eingebettet. Anschließend erfolgt im Schritt 401 eine Abfrage der Eingabemittel auf eventuelle weitere Eingaben. Liegen weitere Eingaben vor wird ein Schleifenzähler im Schritt 403 zurückgesetzt und zum Punkt t (Fig. 3) zurückverzweigt.

Die Eingabedaten, die mit einer Tastatur 2 oder aber über eine an die Ein/Ausgabeeinrichtung 4 angeschlossene, den Portwert errechnende, elektronische Waage 22 eingegeben werden, werden automatisch im Speicherbereich D des nichtflüchtigen Arbeitsspeichers NVM 5 gespeichert. Außerdem sind auch Datensätze der Subspeicherbereiche, zum Beispiel B_j, C usw., nichtflüchtig gespeichert. Damit ist gesichert, daß die letzten Eingabegrößen auch beim Ausschalten der Frankiermaschine erhalten bleiben, so daß nach dem Einschalten automatisch der Portwert im Wertabdruck entsprechend der letzten Eingabe vor dem Ausschalten der Frankiermaschine und das Datum im Tagesstempel entsprechend dem aktuellem Datum vorgegeben wird. Im Schritt 209 wird die eventuelle Eingabe neuer Werte abgefragt. Wenn beispielsweise kein neuer Portwert eingegeben wurde, dann wird auf den im Speicherbereich gespeichert vorliegenden bisherigen Portwert zurückgegriffen und der Punkt e (Fig. 3) erreicht, um weitere Eingaben abzufragen, bevor der Frankiermodus 400 (Fig. 5) erreicht wird.

Bei einer im Schritt 401 festgestellten erneuten Eingabeanforderung wird wieder auf den Schritt 209 zurückverzweigt. Anderenfalls wird auf den Schritt 402 verzweigt, um den Schleifenzähler zu inkrementieren. Über den Schritt 404, in welchen die durchlaufenen Schleifenanzahl überprüft wird, wird der Schritt 405 erreicht, um die Druckausgabeanforderung abzuwarten. Durch einen Briefsensor wird ein Brief detektiert, welcher frankiert werden soll. Dadurch wird ein Signal für die Druckausgabeanforderung generiert.

Im Schritt 405 wird die Druckausgabeanforderung abgewartet, um dann über die Schritte 407, 409 und 410 zur Abrechnungs- und Druckroutine im Schritt 406 zu verzweigen. Liegt keine Druckausgabeanforderung (Schritt 405) vor, wird — nach dem in der Fig. 3 gezeigten Gesamtablaufplan — zum Schritt 209 (Punkt t) und gegebenenfalls, wenn kein Kommunikationsersuchen vorliegt über die Schritte 211, 212 und 214 zum Schritt 401 des Frankiermodus 400 zurückverzweigt.

Wenn nach der — in der Fig. 5 dargestellten — Weise nunmehr zum Punkt t zurückverzweigt und nach Schritt 209 der Schritt 301 erreicht wird, kann jederzeit durch manuelle Eingabe ein Kommunikationsersuchen gestellt oder eine andere Eingabe gemäß den Schritten Testanforderung 212 und Registercheck 214 getätigt werden. Wieder wird Schritt 401 erreicht. Wenn keine Eingabeanforderung erkannt wird, werden weitere Schritte 402 und 404 — wie in der Fig. 5 gezeigt — durchlaufen. Ein weiteres Abfragekriterium kann in einem Schritt 404 abgefragt werden, um im Schritt 408 ein Standby-Flag zu setzen, wenn nach einer durchlaufenen Schleifenanzahl weder eine Eingabe getätigt wurde, noch keine Druck-Ausgabeanforderung vorliegt.

Der Standby-Modus wird in einer anderen Variante auch erreicht, wenn ein an sich bekannter — in der Fig. 1 dargestellter — Briefsensor 16 in vorbestimmter Zeit keinen nächsten Briefumschlag ermittelt, welcher frankiert werden soll. Der — in der Fig. 4 gezeigte — Schritt 404 im Frankiermodus 400 umfaßt entweder eine Abfrage nach einem Zeitablauf oder nach der Anzahl an Durchläufen durch die Programmschleife, welche letztendlich wieder auf die Eingaberoutine gemäß Schritt

401 führt. Wird das Abfragekriterium erfüllt, wird im Schritt 408 ein Standby-Flag gesetzt und direkt auf den Punkt p oder alternativ dazu auf den Punkt s zur Systemroutine 200 zurückverzweigt, ohne daß die Abrechnungs- und Druckroutine im Schritt 406 durchlaufen wird. Bei einer Verzweigung auf den Punkt p kann ein zusätzlicher Wechsel der Codewörter während des Standby-Modus erzielt werden. Bei einer — in der Fig. 5 nicht dargestellte — Variante mit einer Verzweigung auf den Punkt s kann dagegen nur ein Wechsel der Codewörter nur nach dem Einschalten erzielt werden.

Das Standby-Flag wird während der Systemroutine 200 im Schritt 211 abgefragt und gegebenenfalls nach der Checksummenprüfung im Schritt 213 zurückgesetzt, falls kein Manipulationsversuch erkannt wird.

Das Abfragekriterium im Schritt 211 wird dazu um die Frage erweitert, ob das Standby-Flag gesetzt ist, d. h. ob der Standby Modus erreicht ist. In diesem Fall wird einmal auf den Schritt 213 verzweigt. Eine bevorzugte Variante mit Manipulationsüberwachung während des Standby-Modus besteht darin, ein Codewort Y in der bereits beschriebenen Weise zu löschen, wenn ein Manipulationsversuch im Standby-Modus auf vorgenannte Weise im Schritt 213 festgestellt worden ist. Das Fehlen des Codewortes Y wird im Schritt 207 erkannt und dann auf den Schritt 208 verzweigt. Der Vorteil dieses Verfahrens in Verbindung mit dem ersten Modus besteht darin, daß der Manipulationsversuch statistisch im Schritt 213 erfaßt wird.

Somit kann das Standby-Flag im auf den Kommunikationsmodus 300 folgenden Schritt 211 abgefragt werden. Damit wird nicht auf den Frankiermodus 400 verzweigt, bevor nicht die Checksummenprüfung die Vollständigkeit und Gültigkeit aller oder mindestens einiger ausgewählter sicherheitsrelevanter Programme ergeben hat.

Falls eine Druckausgabeanforderung im Schritt 405 erkannt wird, werden weitere Abfragen in den nachfolgenden Schritten 409 und 410 sowie im Schritt 406 getätigt. Beispielsweise kann im Schritt eine Überprüfung der Registerwerte und zusätzlich des Codewortes y vorgenommen werden und im Schritt 409 wird die Gültigkeit und zusätzlich das Vorhandensein eines im Schritt 208 (Fig. 3) gesetzten Kill-Mode-Flag's festgestellt, um auf den Schritt 410 zu verzweigen. Anderenfalls wird auf den Schritt 413 zur Statistik- und/oder Fehlerauswertung und Schritt 415 zur Anzeige des Fehlers verzweigt, wenn die Registerwerte nicht authentisch waren.

Im Schritt 410 wird das Erreichen eines weiteren Stückzahlkriterium abgefragt. War die zum Frankieren vorbestimmte Stückzahl bei der vorhergehenden Frankierung verbraucht, d. h. Stückzahl gleich Null, wird automatisch zum Punkt e verzweigt, um in den Kommunikationsmodus 300 einzutreten, damit von der Datenzentrale eine neue vorbestimmte Stückzahl S wieder kreditiert wird. War jedoch die vorbestimmte Stückzahl noch nicht verbraucht, wird vom Schritt 410 auf die Abrechnungs- und Druckroutine im Schritt 406 verzweigt. Im Schritt 406 werden die in bekannter Weise zur Abrechnung eingezogenen Registerdaten ggf. inhaltlich überprüft und entsprechend geändert. Beispielsweise wird bei einem gültigen Frankieren mit einem Wert > 0 der Stückzähler R4 inkrementiert. Der Registerwert R1 wird verringert und der Registerwert R2 entsprechend erhöht, so daß der Registerwert R3 konstant bleibt. Danach wird eine Prüfsumme (beispielsweise CRC) über jeden der Registerwerte gebildet und im NVM 5a und/oder NVM 5b zusammen mit den zugehörigen Register-

werten gespeichert. Eine solche Absicherung, die über die einzelnen Registerdaten gelegt wurde, um, eine Manipulation Verringeren von R2 (Verbrauchssumme) und Erhöhung von R1 (Restwert) bei gleichbleibenden R3 während des laufenden Betriebes zu verhindern, wurde bereits in der Anmeldung DE 43 44 476 A1 vorgeschlagen. Der MAC (Message Authentication Code) ist eine verschlüsselte Checksumme, welche an den Registerwert bei Abrechnung im Schritt 406 (Fig. 4) angehängt wird. Geeignet ist beispielsweise eine DES-Verschlüsselung. Im Frankiermodus 400 (Fig. 4) kann bei der Abrechnung zusätzlich noch der Dateninhalt überprüft werden, ob die Registerwertsumme R3 gleich der Summe aus Ascending-Register R1 (Restwert) und Descending-Register R2 ist. Aufgrund der Absicherung mit den verschlüsselten Prüfsummen kann aber auf eine inhaltliche Überprüfung völlig verzichtet werden, zumal eine solche von der Datenzentrale bei jeder Kommunikation mit der Frankiermaschine durchgeführt wird. Sind alle Spalten eines Druckbildes gedruckt worden, wird wieder zur Systemroutine 200 zurückverzweigt.

Die Anzahl von gedruckten Briefen, und die aktuellen Werte in den Postregistern werden entsprechend der eingegebenen Kostenstelle im nichtflüchtigen Speicher 5a der Frankiermaschine während der Abrechnungsroutine 406 registriert und stehen für eine spätere Auswertung zur Verfügung. Ein spezieller Sleeping-Mode-Zähler wird während der unmittelbar vor dem Druck erfolgenden Abrechnungsroutine veranlaßt, einen Zähler schritt weiterzuzählen. Die Registerwerte können bei Bedarf im Anzeigemodus 215 (Fig. 3) abgefragt werden. Von diesem wird anschließend zur Systemroutine 200 zurückverzweigt.

Für die frankiermaschineninterne Sicherheitsschaltung eignet sich der TMS370 C010 aus der Prozessorfamilie von Texas Instrument. Dieser weist ein internes E²PROM von 256 Bytes als NVM auf.

In einer Variante enthalten der nichtflüchtige interne Prozessorspeicher und der zu schützende nichtflüchtige Postregisterspeicher (Bat-NV-CMOS-RAM's) nicht das identische, sondern einer von beiden das komplementäre Codewort. Das prozessorinterne Codewort ist nicht von außen abfragbar.

In einer anderen Variante sind verschiedene Codewörter einzelnen Speichern zugeordnet, wobei die verschiedenen Codewörter jedoch einen gemeinsamen Stamm haben, aus dem sie gebildet wurden und wobei der gemeinsame Stamm vom Prozessor rekonstruiert wird, um die Gültigkeit der einzelnen Codewörter zu überprüfen.

Die Routine zum Codewörter-Vergleich bzw. zur Gültigkeitsprüfung wird im Prozessor jeweils nach dem Einschalten bzw. bei Programmfortsetzung abgefragt. Wird beim Vergleich eine Unstimmigkeit festgestellt, wird die Frankiermaschine für den weiteren Betrieb blockiert.

Es ist weiterhin vorgesehen, daß die Anzahl der Bildung von neuen Codewörtern ab einem vorbestimmten Zeitpunkt gezählt und nichtflüchtig prozessorintern gespeichert wird. Zum Zeitpunkt einer Kommunikation mit der Datenzentrale wird die vorgenannte Anzahl an in der Vergangenheit gebildeten Codewörtern und das aktuell gültige Codewort abgefragt. Das erlaubt bei einer unabsichtlichen Blockierung der Frankiermaschine aufgrund ungültiger Codewörter dann bei Bedarf die nachträgliche Wiederherstellung des alten Zustandes durch entsprechende Datenübermittlung seitens der Datenzentrale an die Frankiermaschine.

Es ist vorgesehen, daß ein dem Codewort entsprechender letzter Betriebszustand der Frankiermaschine einen Zustand im Ergebnis der Herstellung oder einer Nachladung der Frankiermaschine oder einen Zustand vor dem Ausschalten der Frankiermaschine oder einen Zustand vor einem Spannungsausfall oder vor einer Stillstandszeit (Stand by) bzw. vor Programmunterbrechung einschließt. Ebenfalls können bei der Überwachung weiterer Kriterien solche letzten Betriebszustände eintreten, indem die Frankiermaschine zu einem entsprechenden Modus übergeht. Solche Schritte 202 bzw. 207 für eine Überwachung weiterer Kriterien weist der in der Fig. 3 dargestellte Gesamtablaufplan für die Frankiermaschine auf. Bei einer Verletzung eines der Sicherheitskriterien tritt die Frankiermaschine in einen entsprechenden Modus ein und führt zusätzlich in entsprechenden Subroutinen die — in der Fig. 7 dargestellten — erfindungsgemäßen Schritte 106 bis 109 aus. Tritt die Frankiermaschine beispielsweise in einen Sleeping-Modus ein, wenn nach Verbrauch einer vorbestimmten Stückzahl noch keine Verbindung zur Datenzentrale aufgenommen wurde, und wird keine manuelle Auslösung einer Kommunikation durch den Nutzer vorgenommen, erfolgt bei Erschöpfung des Stückzahlkredites eine automatische Kommunikation mit der Datenzentrale und eine Durchführung des Verfahrens zur Erhöhung der Manipulationssicherheit von kritischen Registerdaten.

Die Erfindung ist nicht auf die vorliegenden Ausführungsform beschränkt, da offensichtlich weitere andere Anordnungen bzw. Ausführungen des Verfahrens für andere informationsverarbeitende Einrichtungen entwickelt bzw. eingesetzt werden können, die vom gleichen Grundgedanken der Erfindung ausgehend, von den anliegenden Ansprüchen umfaßt werden.

Patentansprüche

1. Verfahren zur Erhöhung der Manipulationssicherheit von kritischen Daten, insbesondere von Registerdaten in Frankiermaschinen, gekennzeichnet durch die Schritte:

- Laden einer Zahl oder eines Zeigers, welcher einem Codewort zugeordnet ist, in einen ersten nichtflüchtigen Speicher 20,
- Laden eines Codewortes in zweite die Postregisterdaten enthaltenden nichtflüchtigen Speicher (NVM 5a, 5b), wobei das Codewort dem letzten Betriebszustand der Frankiermaschine zugeordnet ist, d. h. das dem Ergebnis der Herstellung oder einer Nachladung der Frankiermaschine bzw. vor dem Ausschalten bzw. vor Spannungsausfall oder vor einer Stillstandszeit (Stand by) bzw. vor Programmunterbrechung entsprechend ausgewählt worden ist,
- Gültigkeitsprüfung des Codewortes mindestens zum Zeitpunkt des Einschaltens der Frankiermaschine und
- Ersetzen des alten Codewortes durch ein vorbestimmtes neues Codewort, wenn der Prozessor, nach Gültigkeitsprüfung mit Bezug auf das in seinem internen Prozessorspeicher (NVM 6c) aus einer Liste mit gespeicherten Codewörtern entsprechend der Zahl bzw. der Zeigerstellung ausgewählte Codewort, die Gültigkeit des alten Codewortes erkennt oder
- Blockierung der Frankiermaschine nach

dem Zeitpunkt des Einschaltens der Frankiermaschine, wenn der Prozessor nach Gültigkeitsprüfung mit Bezug auf das ausgewählte in vorgenannter Liste gespeicherte Codewort die Gültigkeit des alten Codewortes aberkennt.

2. Verfahren, nach Anspruch 1, dadurch gekennzeichnet, daß ein dem Codewort entsprechender letzter Betriebszustand der Frankiermaschine einen Zustand im Ergebnis der Herstellung oder einer Nachladung der Frankiermaschine oder einen Zustand vor dem Ausschalten der Frankiermaschine oder einen Zustand vor einem Spannungsausfall oder vor einer Stillstandszeit (Stand by) bzw. vor Programmunterbrechung einschließt.
3. Verfahren, nach Anspruch 2, dadurch gekennzeichnet, daß die Nachladung mit einem monetären Guthaben, Stückzahl S und/oder anderen Daten in einem Kommunikationsmodus (300) erfolgt, daß die Anzahl der Bildung von neuen Codewörtern ab einem vorbestimmten Zeitpunkt gezählt und nichtflüchtig prozessorextern gespeichert wird und zum Zeitpunkt einer Kommunikation mit der Datenzentrale die vorgenannte Anzahl an in der Vergangenheit gebildeten Codewörtern und das aktuell gültige Codewort abgefragt wird, zum Überwinden einer unabsichtlichen Blockierung der Frankiermaschine aufgrund ungültiger Codewörter bzw. bei Bedarf die nachträgliche Wiederherstellung des alten Zustandes durch entsprechende Datenübermittlung seitens der Datenzentrale an die Frankiermaschine.
4. Verfahren, nach Anspruch 2, dadurch gekennzeichnet, daß eine Überwachung weiterer Kriterien erfolgt und solche vorgenannten letzten Betriebszustände eintreten, indem die Frankiermaschine zu einem entsprechenden Modus bei einer Verletzung eines der Sicherheitskriterien übergeht, daß die in einen entsprechenden Modus eingetretene Frankiermaschine in zusätzlichen entsprechenden Subroutinen die Schritte (106 bis 109) zur Durchführung des Verfahrens zur Erhöhung der Manipulationssicherheit von kritischen Registerdaten ausführt.
5. Verfahren, nach Anspruch 1, dadurch gekennzeichnet, daß für zwei nichtflüchtige Speicher NVM 20 und NVM 5a nach Überprüfung des alten Codewortes im Schritt 107 und vor der entsprechenden Veränderung von Codewörtern V und U zunächst im Schritt 108 ein neues Codewort W' und danach ein Codewort T' gebildet wird, nach den Gleichungen:

$$\begin{aligned} W' &:= F\{P1\} \text{ und } (1) \\ T' &:= F\{P2\}, \quad (2) \end{aligned}$$

wobei P1 und P2 gelistete Codewörter sind.

6. Verfahren, nach Anspruch 5, dadurch gekennzeichnet, daß im internen NVM 20 ein Zählwert inkrementiert, dekrementiert oder in vorbestimmter Weise verändert wird, bevor ein neues Codewort (W', T', U', V') gebildet wird.
7. Verfahren, nach Anspruch 1, dadurch gekennzeichnet, daß die Bildung des neuen Codewort vom vorherigen abhängig ist.
8. Verfahren, nach Anspruch 1, dadurch gekennzeichnet, daß ein Laden eines neuen Codewortes in zu schützende nichtflüchtige Speicher (NVM 5a, 5b), erfolgt, wobei das Programm für die Berech-

nung der Zeigerstellung bzw. Bildung des jeweils neuen Codewortes im Programmspeicher (PSP 11) gespeichert ist.

9. Verfahren, nach Anspruch 8, dadurch gekennzeichnet, daß als Programmspeicher ein ROM bzw. EPROM verwendet wird.
10. Verfahren zur Erhöhung der Manipulationssicherheit von kritischen Daten, dadurch gekennzeichnet, daß jedem nichtflüchtigem Speicher oder Speicherbereich ein separates Codewort zugeordnet wird, wobei mindestens eines der vorgenannten separaten Codeworte in einem weiteren internen Speicher eines Prozessorsystems, einer Chipkarte und/oder einer Datenzentrale nichtflüchtig gespeichert worden ist und daß eine Bildung von neuen Codewörtern ab einem vorbestimmten Zeitpunkt und danach eine Einspeicherung der neuen Codewörter in die zu schützenden nichtflüchtigen Speicher vorgenommen wird.
11. Verfahren, nach Anspruch 10, dadurch gekennzeichnet, daß die Bildung des neuen Codewortes vom vorherigen abhängig ist.
12. Verfahren, nach Anspruch 10, dadurch gekennzeichnet, daß in einem Schritt (108) zur Bildung eines neuen veränderbaren ersten Codewortes (T', W') auch die Bildung des neuen zweiten Codewortes (V', U') identisch zur Bildung des neuen ersten Codewortes (T', W') erfolgt, um ein identisches neues zweites Codewort (V', U') in die zu schützenden nichtflüchtigen Speicher (NVMs 5a, 5b) zu laden, oder daß in einem Schritt (108) zur Bildung eines neuen veränderbaren ersten Codewortes (T', W') auch die Bildung des neuen zweiten Codewortes (V'', U'') als komplementärer Schatten (V'', U'') zum neuen ersten Codewortes (T', W') erfolgt, um ein komplementäres neues zweites Codewort (V', U') in die zu schützenden nichtflüchtigen Speicher (NVMs 5a, 5b) zu laden.
13. Verfahren, nach Anspruch 10, dadurch gekennzeichnet, daß in einem Schritt (108) zur Bildung eines neuen veränderbaren ersten Codewortes (T', W') auch die Bildung des neuen zweiten Codewortes (V', U'') als zu dem veränderbaren neuen ersten Codewort (W') identischen Codewort (V') und als komplementärer Schatten (U'') zum neuen ersten Codewortes (T') erfolgt, um mindestens ein neues zweites Codewort (V', U'') in die zu schützenden nichtflüchtigen Speicher (NVMs 5a, 5b) zu laden oder daß beim Schutz eines entsprechenden Speichers (NVM's) in mindestens einem der Speicherbereiche auch mit dem komplementären Schatten (V'' oder U'') gearbeitet wird.
14. Verfahren, nach Anspruch 10, dadurch gekennzeichnet, daß eine Nachladung mit einem monetären Guthaben, Stückzahl S und/oder anderen Daten in einem Kommunikationsmodus (300) erfolgt, daß die Anzahl der Bildung von neuen Codewörtern ab einem vorbestimmten Zeitpunkt gezählt und nichtflüchtig prozessorextern gespeichert wird und zum Zeitpunkt einer Kommunikation mit einer Datenzentrale die vorgenannte Anzahl an in der Vergangenheit gebildeten Codewörtern und das aktuell gültige Codewort abgefragt wird, zum Überwinden einer unabsichtlichen Blockierung der Frankiermaschine aufgrund ungültiger Codewörter bzw. zur bedarfsweisen nachträglichen Wiederherstellung des alten Zustandes durch entsprechende Datenübermittlung seitens der Datenzentrale an

die Frankiermaschine.

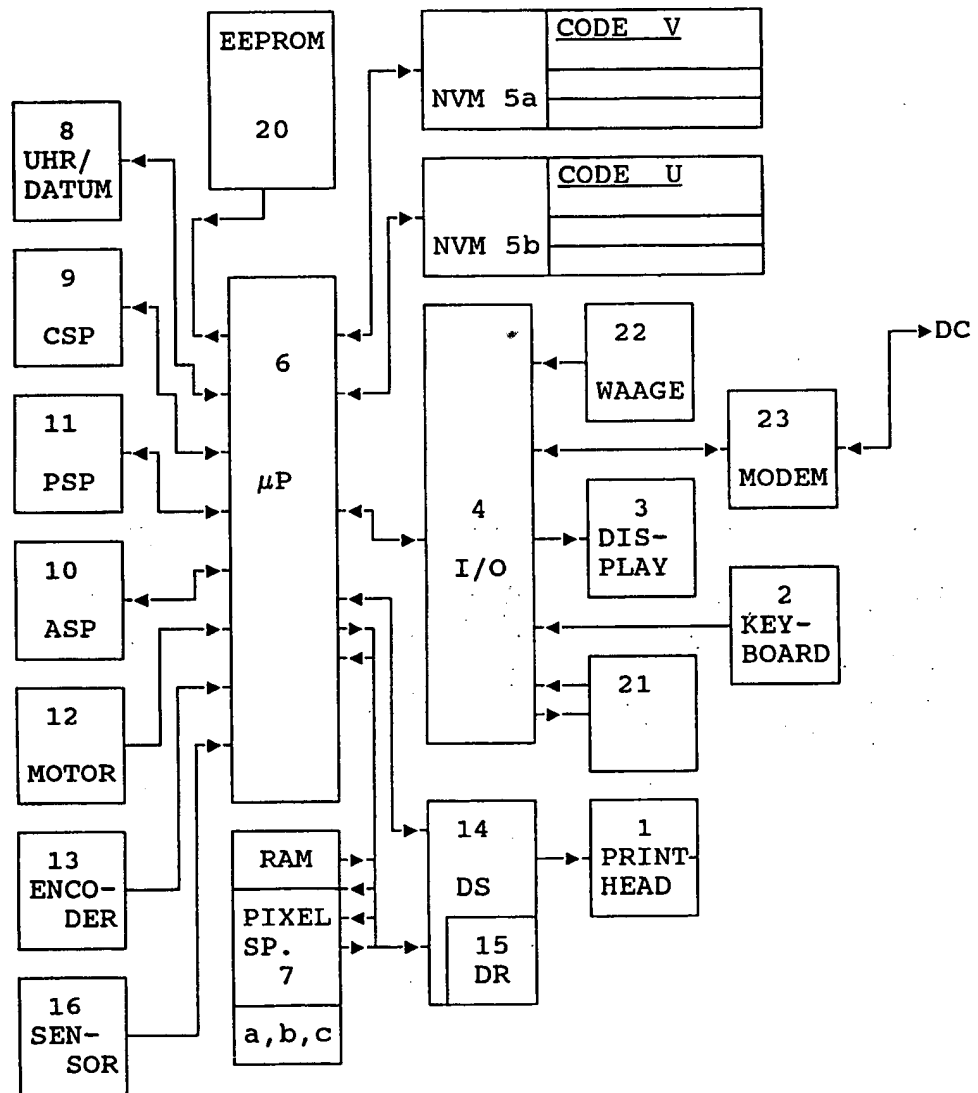
15. Verfahren zur Erhöhung der Manipulationssicherheit von kritischen Daten in informationsverarbeitenden Einrichtungen, gekennzeichnet, durch die Schritte:

- Laden einer Zahl oder eines Zeigers, welcher einem Codewort zugeordnet ist, in einen ersten nichtflüchtigen Speicher (20),
- Laden eines Codewortes in zweite die Postregisterdaten enthaltenden nichtflüchtigen Speicher (NVM 5a, 5b), wobei das Codewort dem letzten Betriebszustand der informationsverarbeitenden Einrichtung zugeordnet ist,
- Gültigkeitsprüfung des Codewortes mindestens zum Zeitpunkt des Einschaltens der informationsverarbeitenden Einrichtung und
- Ersetzen des alten Codewortes durch ein vorbestimmtes neues Codewort, wenn der Prozessor, nach Gültigkeitsprüfung mit Bezug auf das in seinem internen Prozessorspeicher (NVM 6c) aus einer Liste mit gespeicherten Codewörtern entsprechend der Zahl bzw. der Zeigerstellung ausgewählte Codewort, die Gültigkeit des alten Codewortes erkennt oder
- Blockierung der informationsverarbeitenden Einrichtung nach dem Zeitpunkt des Einschaltens, wenn der Prozessor nach Gültigkeitsprüfung mit Bezug auf das ausgewählte in vorgenannter Liste gespeicherte Codewort die Gültigkeit des alten Codewortes aberkennt.

16. Anordnung zur Erhöhung der Manipulationssicherheit von kritischen Daten, insbesondere von Registerdaten in Frankiermaschinen mit einer Steuereinrichtung und Speichern, dadurch gekennzeichnet, daß die Steuereinrichtung (6) einen Mikroprozessor oder einen OTP-Prozessor (ONE TIME PROGRAMMABLE) aufweist, in welchem neben einem Mikroprozessor CPU (6a) auch weitere Schaltungen und/oder Programme bzw. Daten im internen OTP-ROM (6c) bzw. im internen OTP-RAM (6b) in einem gemeinsamen Bauelementgehäuse untergebracht sind, welche ein erstes Sicherheitsmittel gegen unbefugte Manipulation bilden sowie daß ein externer nichtflüchtiger Speicher NVM (20) ein zweites Sicherheitsmittel gegen unbefugte Manipulation bildet.

Hierzu 6 Seite(n) Zeichnungen

- Leerseite -

**Fig. 1**

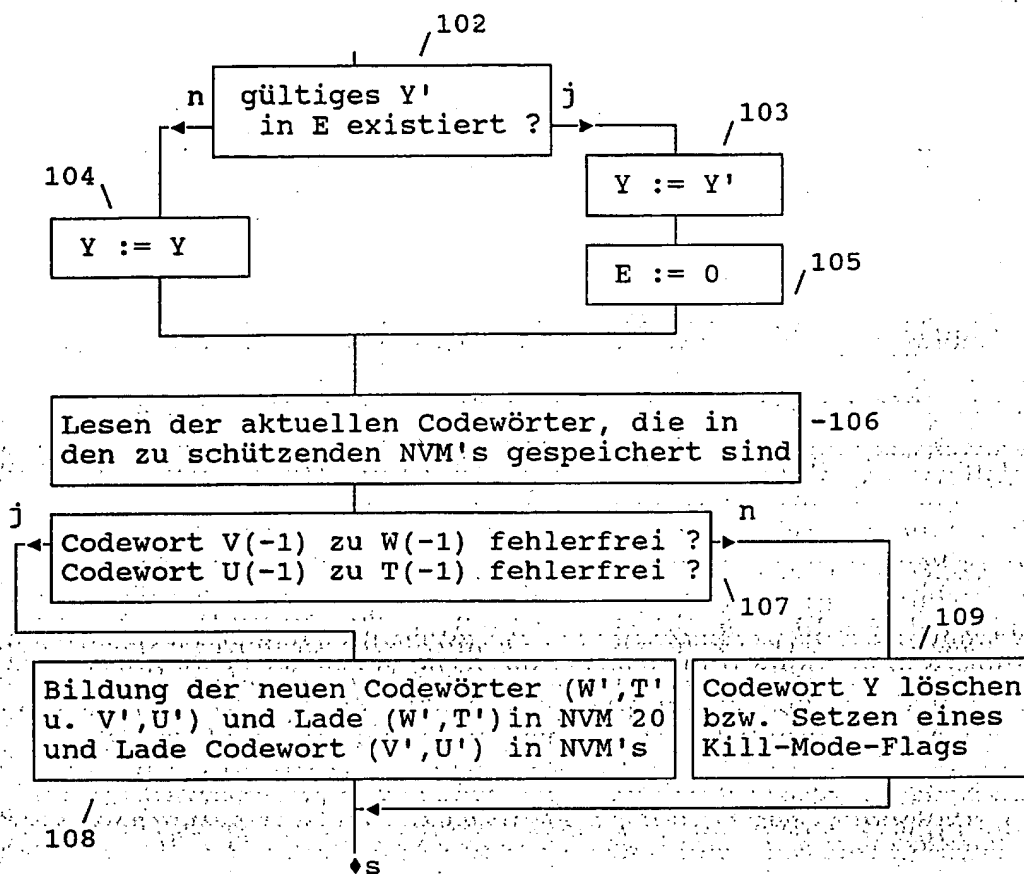


Fig. 7

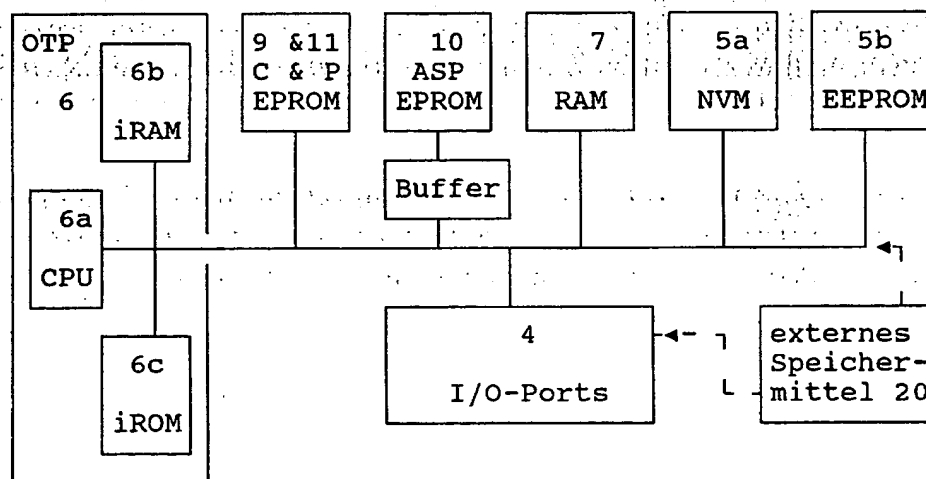


Fig. 2

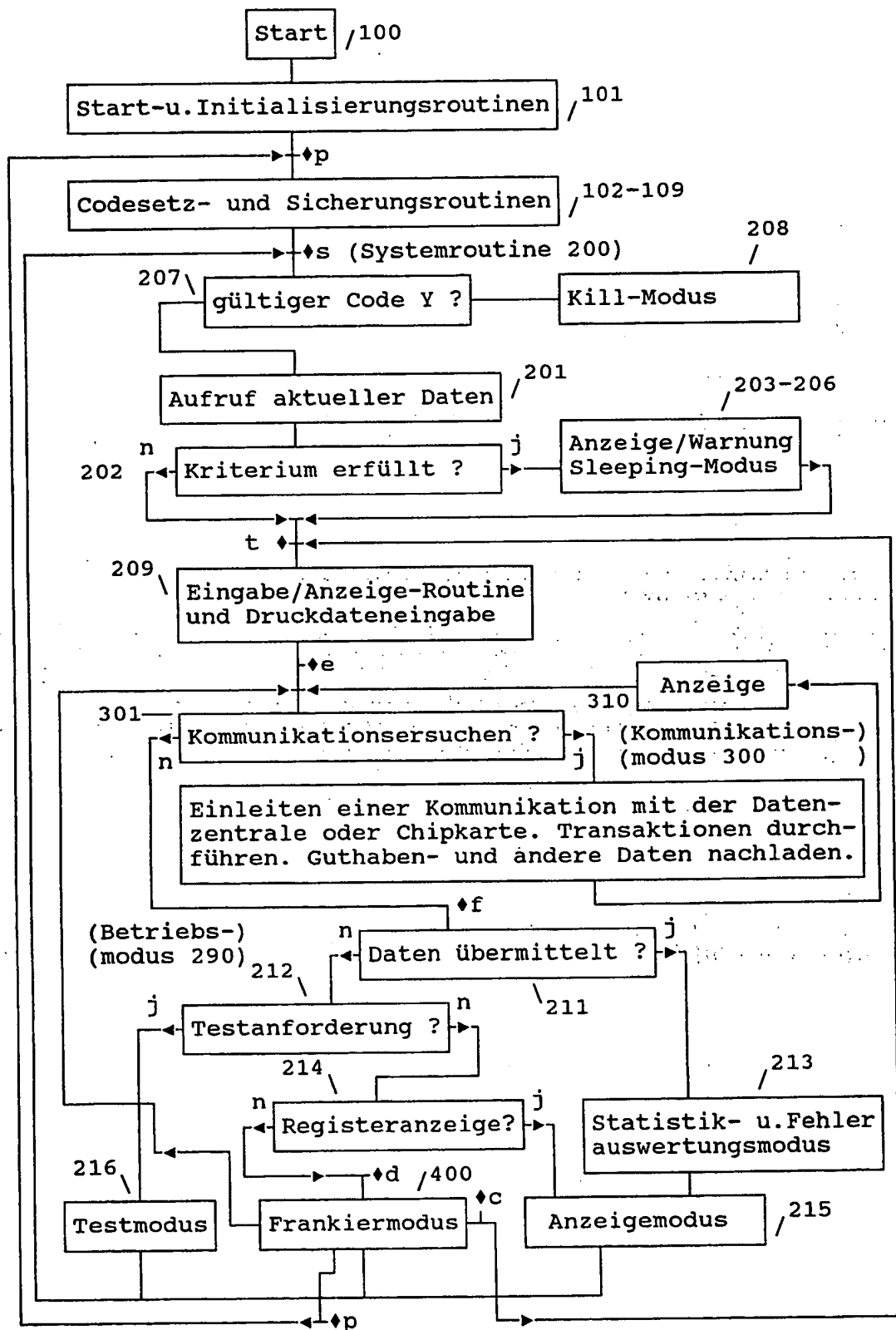
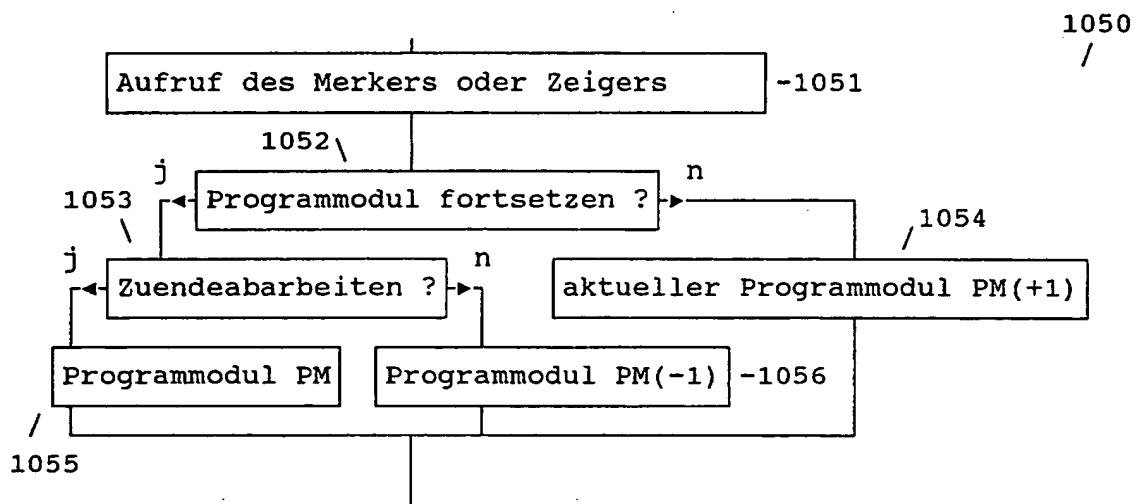
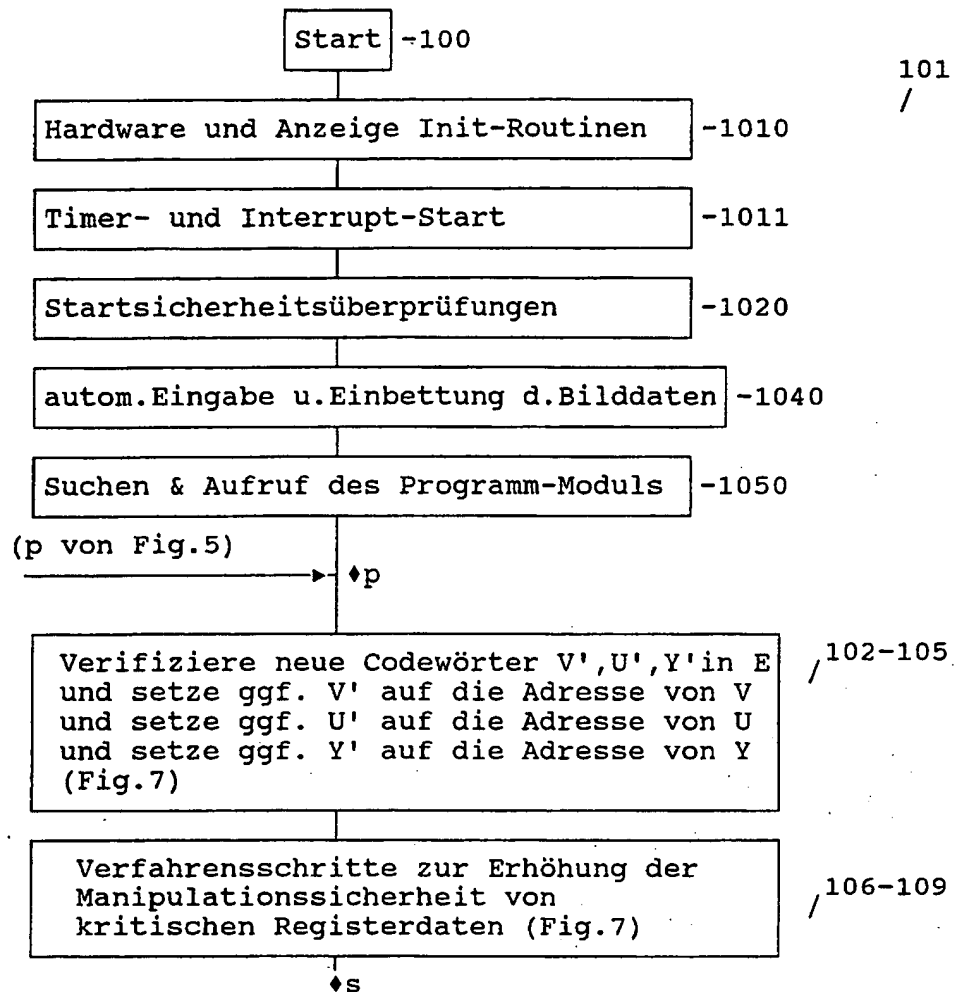


Fig. 3



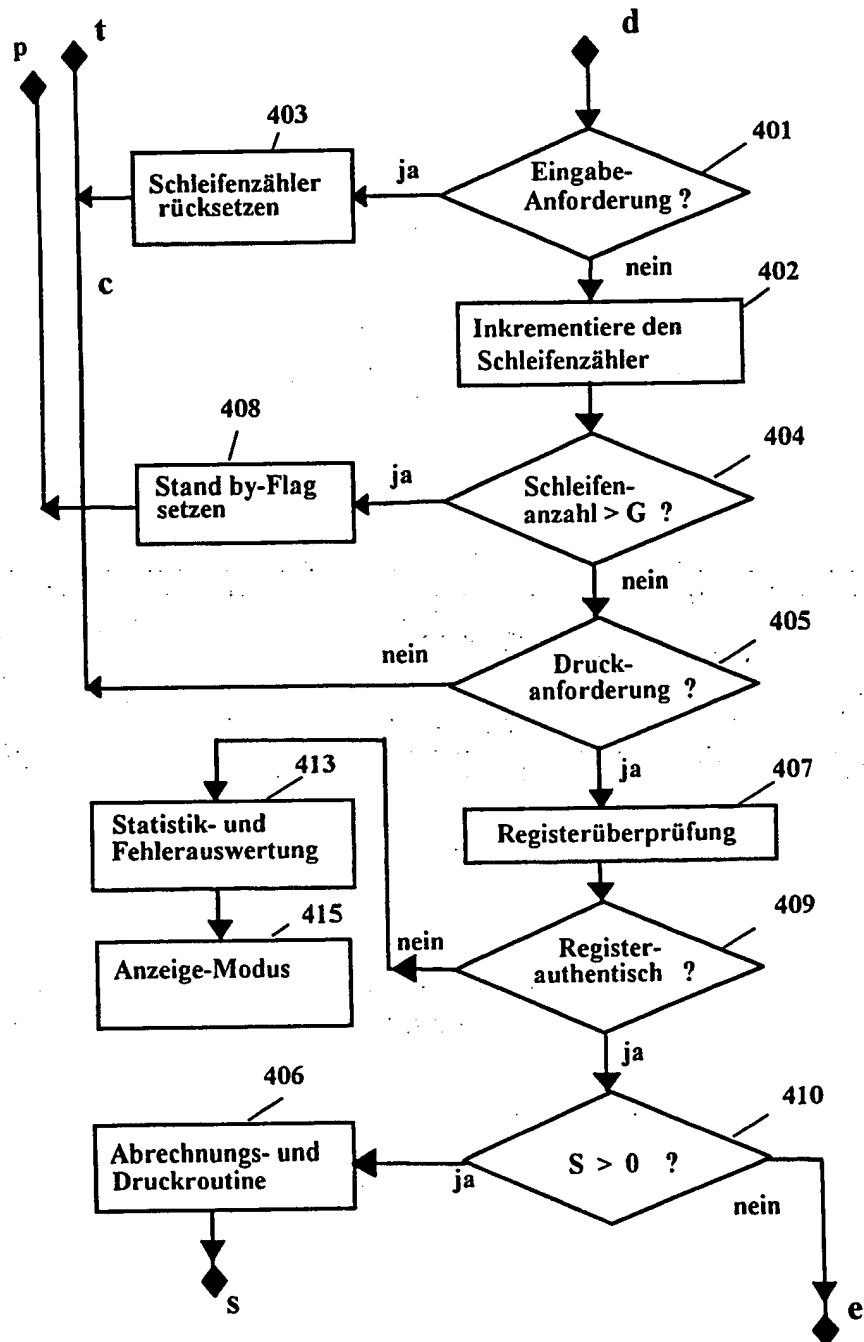
**Fig. 5**

Fig. 8a

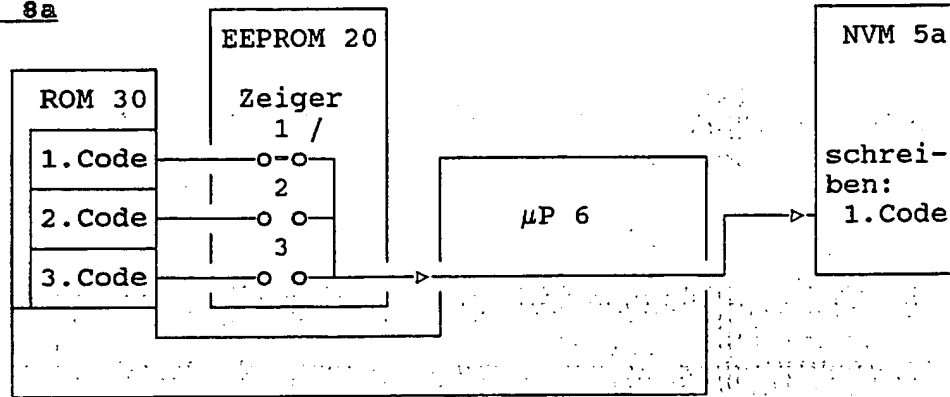


Fig. 8b

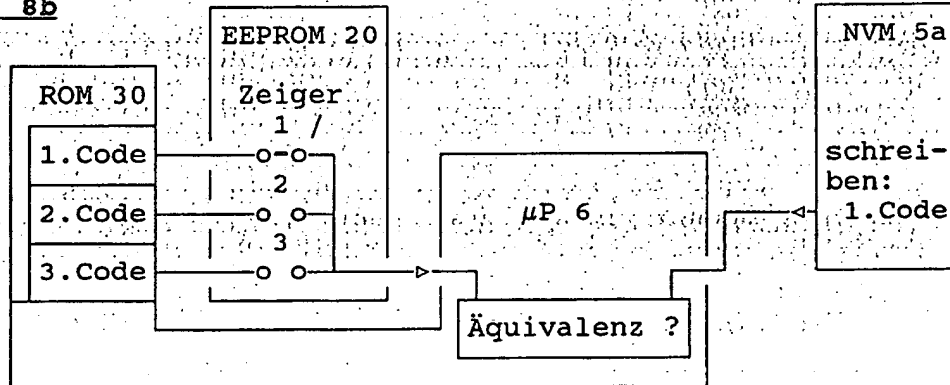
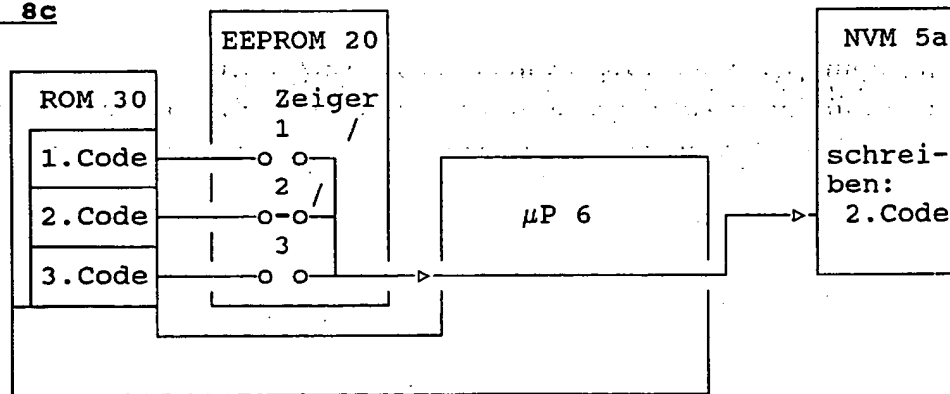


Fig. 8c



Docket # GTP/US 3183

Applic. # 09/917,541

Applicant: Reisinger

Lerner and Greenberg, P.A.

Post Office Box 2480

Hollywood, FL 33022-2480

Tel: (954) 925-1100 Fax: (954) 925-1101